Kaspersky Internet Security 2011

Benutzerhandbuch

PROGRAMMVERSION: 11.0 CRITICAL FIX 2

Sehr geehrter Benutzer!

Vielen Dank, dass Sie unser Produkt ausgewählt haben. Wir hoffen, dass diese Dokumentation Ihnen hilft und die meisten Fragen damit beantwortet werden können.

Achtung! Jedwedes Kopieren, Weiterbreiten oder zum Beispiel Übersetzen von Unterlagen wird nur schriftlich von Kaspersky Lab genehmigt.

Das Dokument und dazu gehörende Grafiken dürfen nur zu informativen, nicht gewerblichen oder persönlichen Zwecken gebraucht werden.

Kaspersky Lab behält sich das Recht vor, dieses Dokument ohne vorherige Benachrichtigung zu ändern. Die neueste Version finden Sie auf der Seite von Kaspersky Lab unter der Adresse http://www.kaspersky.de/docs.

Für den Inhalt, die Qualität, Aktualität und Richtigkeit der im Dokument verwendeten Unterlagen, deren Rechte anderen Rechteinhabern gehören, sowie für den möglichen Schaden durch die Nutzung dieser Unterlagen, lehnt Kaspersky Lab die Haftung ab.

In diesem Dokument werden eingetragene Markenzeichen und Handelsmarken verwendet, die das Eigentum der jeweiligen Rechteinhaber sind.

Redaktionsdatum: 08.09.2010

© 1997-2010 Kaspersky Lab ZAO. Alle Rechte vorbehalten.

http://www.kaspersky.de
http://support.kaspersky.de

INHALT

ENDNUTZER-LIZENZVERTRAG FÜR KASPERSKY LAB SOFTWARE 12

ÜBER DIESES HANDBUCH 19

In diesem Dokument 19

Formatierung mit besonderer Bedeutung 20

ZUSÄTZLICHE INFORMATIONSQUELLEN 22

Informationsquellen zur selbständigen Recherche 22

Diskussion über die Programme von Kaspersky Lab im Webforum 23

Kontaktaufnahme mit der Vertriebsabteilung 23

Kontakt zur Abteilung für Handbücher und Hilfesysteme 23

KASPERSKY INTERNET SECURITY 2011 24

Neuerungen 24

Organisation des Schutzes für Ihren Computer 25

Lieferumfang 27

Service für registrierte Benutzer 27

Hard- und Softwarevoraussetzungen 28

PROGRAMM INSTALLIEREN UND DEINSTALLIEREN 29

Standard-Installationsmethode 29

Schritt 1. Nach neuer Programmversion suchen 30

Schritt 2. Systemkompatibilität für Installation prüfen 30

Schritt 3. Installationstyp wählen 31

Schritt 4. Lizenzvereinbarung anzeigen 31

Schritt 5. Erklärung zur Verwendung von Kaspersky Security Network 31

Schritt 6. Inkompatible Programme suchen 31

Schritt 7. Installationsverzeichnis wählen 32

Schritt 8. Installation vorbereiten 32

Schritt 9. Installation 33

Schritt 10. Programm aktivieren 33

Schritt 11. Anmeldung des Benutzers 34

Schritt 12. Aktivierung abschließen 34

Schritt 13. Systemanalyse 34

Schritt 14. Assistent abschließen 34

Aktualisierung einer Vorgängerversion von Kaspersky Internet Security 34

Schritt 1. Nach neuer Programmversion suchen 35

Schritt 2. Systemkompatibilität für Installation prüfen 36

Schritt 3. Installationstyp wählen 36

Schritt 4. Lizenzvereinbarung anzeigen 36

Schritt 5. Erklärung zur Verwendung von Kaspersky Security Network 36

Schritt 6. Inkompatible Programme suchen 37

Schritt 7. Installationsverzeichnis wählen 37

Schritt 8. Installation vorbereiten 38

Schritt 9. Installation 38

Schritt 10. Aktivierung abschließen 38

Schritt 11. Systemanalyse 39

Schritt 12. Assistent abschließen 39

Untypische Installationsszenarien 39
Erste Schritte 40
Programm deinstallieren. 40
Schritt 1. Daten zur erneuten Verwendung speichern 40
Schritt 2. Programmdeinstallation bestätigen 41
Schritt 3. Programm deinstallieren. Deinstallation abschließen 41
LIZENZVERWALTUNG 42
Über den Lizenzvertrag 42
Über die Lizenz 42
Über den Aktivierungscode 43
Lizenz-Info anzeigen 44
PROGRAMMOBERFLÄCHE 45
Symbol im Infobereich der Taskleiste 45
Kontextmenü 46
Hauptfenster von Kaspersky Internet Security 47
Meldungsfenster und Popupmeldungen 50
Programmkonfigurationsfenster 52
Kaspersky Gadget 53
PROGRAMM STARTEN UND BEENDEN 54
Automatischen Start aktivieren und deaktivieren 54
Programm manuell starten und beenden 54
SCHUTZSTATUS DES COMPUTERS 55
Probleme im Computerschutz diagnostizieren und beheben 55
Schutz aktivieren und deaktivieren 57
Schutz anhalten und fortsetzen 58
LÖSUNGEN FÜR TYPISCHE AUFGABEN 60
Wie wird das Programm aktiviert? 60
Lizenzerwerb oder -verlängerung 61
Was tun, wenn das Programm Meldungen anzeigt? 62
Aktualisierung von Programmdatenbanken und -modulen 62
Wie wichtige Computerbereiche auf Viren untersucht werden. 63
Untersuchung von Dateien, Ordnern, Laufwerken und anderen Objekten auf Viren 64
Wie eine vollständige Virenuntersuchung des Computers ausgeführt wird. 65
Wie der Computer auf Schwachstellen untersucht wird. 66
Wie Ihre persönlichen Daten vor Diebstahl geschützt werden 67
Schutz vor Phishing 67
Virtuelle Tastatur 68
Was tun, wenn Sie vermuten, dass ein Objekt von einem Virus infiziert ist? 69
Wie mit einer großen Anzahl von Spam-Mails verfahren wird? 70
Was tun, wenn Sie vermuten, dass Ihr Computer infiziert ist? 71
Wie ein Objekt wiederhergestellt wird, das vom Programm gelöscht oder desinfiziert wurde. 72
Wie eine Notfall-CD erstellt und verwendet wird. 73
Notfall-CD erstellen 73
Hochfahren eines Computers mit Hilfe der Notfall-CD 75
Aufrufen des Berichts über die Programmaktivität 76
Wie werden die Standardeinstellungen des Programms wiederhergestellt? 76
Wie Programmeinstellungen von Kaspersky Internet Security auf einen anderen Computer übertragen werden. 78

Wie das Kaspersky Gadget verwendet wird. 78
ERWEITERTE PROGRAMMEINSTELLUNGEN 81
Grundlegende Schutzparameter 82
Kontrolle des Zugriffs auf Kaspersky Internet Security. 83
Schutzmodus wählen 83
Untersuchung des Computers 84
Virensuche 84
Sicherheitsstufe ändern und wiederherstellen 86
Zeitplan für den Untersuchungsstart erstellen 86
Liste der Untersuchungsobjekte erstellen 87
Untersuchungsmethode wählen 88
Untersuchungstechnologien wählen 88
Aktion beim Fund einer Bedrohung ändern 88
Untersuchungsstart mit den Rechten eines anderen Benutzers 89
Typ der zu untersuchenden Objekte ändern 89
Untersuchung von zusammengesetzten Dateien 90
Untersuchung optimieren 90
Wechseldatenträger beim Anschließen untersuchen 91
Verknüpfung für den Aufgabenstart erstellen 91
Suche nach Schwachstellen 92
Update 92
Updatequelle auswählen 93
Region des Updateservers wählen 94
Update aus dem gemeinsamen Ordner 94
Zeitplan für Updatestart erstellen 95
Rollback zum vorherigen Update 96
Untersuchung der Quarantäne nach dem Update 96
Proxyserver verwenden 96
Updatestart mit den Rechten eines anderen Benutzers 97
Datei-Anti-Virus 97
Datei-Anti-Virus aktivieren und deaktivieren 98
Datei-Anti-Virus automatisch anhalten 98
Schutzbereich festlegen 99
Sicherheitsstufe ändern und wiederherstellen 100
Untersuchungsmodus wählen 100
Heuristische Analyse verwenden 101
Untersuchungstechnologien wählen 101
Aktion für gefundene Objekte ändern 101
Untersuchung von zusammengesetzten Dateien 102
Untersuchung optimieren 103
Mail-Anti-Virus 103
Mail-Anti-Virus aktivieren und deaktivieren 104
Schutzbereich festlegen 105
Sicherheitsstufe ändern und wiederherstellen 105
Heuristische Analyse verwenden 106
Aktion für gefundene Objekte ändern 106
Anlagenfilterung 106
Untersuchung von zusammengesetzten Dateien 107

E-Mail-Untersuchung in Microsoft Office Outlook 107
E-Mail-Untersuchung in The Bat! 107
Web-Anti-Virus 108
Web-Anti-Virus aktivieren und deaktivieren 110
Sicherheitsstufe für Web-Anti-Virus wählen 111
Aktionen für gefährliche Objekte wählen 111
Link-Untersuchung mit den Datenbanken für verdächtige und Phishing-Adressen 112
Heuristische Analyse verwenden 112
Gefährliche Skripts blockieren 113
Untersuchung optimieren 113
Modul zur Link-Untersuchung 114
Zugriff auf gefährliche Webseiten blockieren 115
Zugriff auf regionale Domains kontrollieren 115
Zugriff auf Online-Banking-Dienste kontrollieren 116
Liste mit vertrauenswürdigen Adressen erstellen 116
Einstellungen für Web-Anti-Virus wiederherstellen 116
IM-Anti-Virus 117
IM-Anti-Virus aktivieren und deaktivieren 117
Schutzbereich festlegen 118
Untersuchungsmethode auswählen 118
Proaktiver Schutz 119
Proaktiven Schutz aktivieren und deaktivieren 119
Gruppe mit vertrauenswürdigen Programmen erstellen 120
Liste der gefährlichen Aktivität verwenden 120
Kontrollregel für gefährliche Aktivität ändern 120
Aktivitätsmonitor 121
Aktivitätsmonitor aktivieren und deaktivieren 121
Vorlagen für gefährliches Verhalten verwenden (BSS) 122
Rollback von Aktionen eines schädlichen Programms 122
Programmkontrolle 123
Programmkontrolle aktivieren und deaktivieren 123
Programme zu Sicherheitsgruppen zuordnen 124
Aktivität von Programmen anzeigen 125
Sicherheitsgruppe ändern und Standardgruppe wiederherstellen 125
Arbeit mit den Regeln der Programmkontrolle 126
Gruppenregeln ändern 126
Programmregeln ändern 127
Herunterladen von Regeln aus dem Kaspersky Security Network 128
Vererbung von Beschränkungen eines übergeordneten Prozesses 129
Regeln für nicht verwendete Programme löschen 129
Schutz für Betriebssystemressourcen und persönliche Daten 130
Interpretation von Daten über die Verwendung eines Programms durch die KSN-Teilnehmer 131
Netzwerkschutz 132
Firewall 132
Firewall aktivieren und deaktivieren 133
Netzwerkstatus ändern 133
Arbeit mit den Firewall-Regeln 133
Benachrichtigungen über Veränderungen eines Netzwerks anpassen 136
Erweiterte Einstellungen für die Firewall 136

Schutz vor Netzwerkangriffen 137
Arten der erkennbaren Netzwerkangriffe 137
Schutz vor Netzwerkangriffen aktivieren und deaktivieren 138
Parameter für das Blockieren ändern 139
Untersuchung geschützter Verbindungen 139
Untersuchung geschützter Verbindungen in Mozilla Firefox 140
Untersuchung geschützter Verbindungen in Opera 141
Netzwerkmonitor 141
Proxyserver-Einstellungen 142
Liste der zu kontrollierenden Ports erstellen 142
Anti-Spam 143
Anti-Spam aktivieren und deaktivieren 145
Stufe für Spam-Schutz wählen 146
Anti-Spam-Training 146
Trainingsassistent verwenden 147
Anti-Spam-Training mit ausgehenden E-Mails 147
Elemente der Benutzeroberfläche eines Mailprogramms verwenden 148
Adressen zur Liste der erlaubten Absender hinzufügen 148
Training mit Berichten 149
Links in Nachrichten untersuchen 149
Spam nach Phrasen und Adressen ermitteln. Listen erstellen 150
Verbotene und erlaubte Phrasen 151
Anstößige Phrasen 152
Verbotene und erlaubte Absender 152
Ihre Adressen 153
Phrasen und Adressen exportieren und importieren 153
Grenzwerte für den Spam-Faktor regulieren 155
Zusätzliche Merkmale, die den Spam-Faktor beeinflussen, verwenden 155
Algorithmus zur Spam-Erkennung wählen 156
Markierung zum Betreff einer Nachricht hinzufügen 156
Nachrichten für Microsoft Exchange Server von der Untersuchung ausschließen 157
Spam-Verarbeitung in Mailprogrammen anpassen 157
Microsoft Office Outlook 158
Microsoft Outlook Express (Windows Mail) 158
Regel für die Spam-Untersuchung von Nachrichten erstellen 158
The Bat! 159
Thunderbird 160
Empfohlene Einstellungen für Anti-Spam wiederherstellen 160
Anti-Banner 160
Anti-Banner aktivieren und deaktivieren 161
Untersuchungsmethoden wählen 162
Listen für verbotene und erlaubte Banneradressen erstellen 162
Adressenlisten exportieren / importieren 162
Sichere Umgebung 163
Sicherer Programmstart 164
Bestimmtes Programm in Sicherer Umgebung starten 165
Arbeit auf dem sicheren Desktop starten und beenden 165
Zwischen normalem Desktop und Sicherer Umgebung wechseln 166
Popup-Symbolleiste verwenden 166

Automatischer Start von Programmen 167
Gemeinsamen Ordner verwenden 167
Sichere Umgebung für Programme bereinigen 168
Sicherer Browser 168
Sicheren Browser starten 169
Browser nach Verwendung des Sicheren Browsers bereinigen 169
Kindersicherung 169
Kindersicherung für einen Benutzer anpassen 170
Benutzerkontrolle aktivieren und deaktivieren 171
Parameter der Kindersicherung exportieren / importieren 172
Darstellung eines Benutzerkontos in Kaspersky Internet Security 173
Arbeitszeit auf dem Computer 174
Start von Programmen 174
Arbeitszeit im Internet 174
Besuch von Webseiten 175
Download von Dateien aus dem Internet 175
Korrespondenz über Instant Messenger 176
Korrespondenz in sozialen Netzwerken 177
Senden vertraulicher Informationen 178
Suche nach Schlüsselwörtern 178
Berichte über die Aktionen eines Benutzers anzeigen 179
Vertrauenswürdige Zone 179
Liste mit vertrauenswürdigen Programmen erstellen 180
Ausnahmeregeln erstellen 181
Leistung und Kompatibilität mit anderen Programmen 181
Kategorien der erkennbaren Bedrohungen wählen 182
Technologie zur Desinfektion einer aktiven Infektion 182
Verteilung der Computerressourcen bei der Virensuche 183
Aufgabenstart im Hintergrundmodus 183
Programmparameter bei der Arbeit im Vollbildmodus. Profil für Spiele 184
Energiesparen im Akkubetrieb 184
Selbstschutz für Kaspersky Internet Security 185
Selbstschutz aktivieren und deaktivieren 185
Schutz vor externer Steuerung 185
Quarantäne und Backup 186
Quarantäne- und Backup-Objekte speichern 186
Arbeit mit Objekten in der Quarantäne 187
Zusätzliche Schutz-Tools 188
Aktivitätsspuren löschen 189
Browser-Konfiguration 191
Rollback von Änderungen, die von den Assistenten ausgeführt wurden 192
Berichte 193
Bericht für eine bestimmte Komponente erstellen 194
Datenfilterung 194
Suche nach Ereignissen 195
Bericht in Datei speichern 196
Berichte speichern 196
Berichte leeren 196
Nicht kritische Ereignisse protokollieren 197

Erinnerung an die Bereitschaft eines Berichts anpassen 197
Aussehen des Programms 197
Grafische Oberfläche von Kaspersky Internet Security 198
Aktive Elemente der Benutzeroberfläche 198
News Agent 198
Meldungen 199
Benachrichtigungen aktivieren und deaktivieren 199
Benachrichtigungsmethode anpassen 200
Teilnahme an Kaspersky Security Network 201
EINSTELLUNGEN VON KASPERSKY INTERNET SECURITY AUF KORREKTHEIT PRÜFEN 202
EICAR-"Testvirus" und seine Modifikationen 202
Testen des Schutzes für HTTP-Datenverkehr 204
Schutz für den SMTP-Datenverkehr testen 204
Überprüfung der Einstellungen von Datei-Anti-Virus 204
Überprüfung der Einstellungen für eine Aufgabe zur Virensuche 205
Überprüfung der Einstellungen für den Schutz vor unerwünschten E-Mails 205
KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT 206
Mein Kaspersky Account 206
Technischer Support am Telefon 207
Bericht über den Systemzustand erstellen 207
Protokolldatei erstellen 208
Dateien mit Daten senden 208
AVZ-Skript ausführen 209
ANHÄNGE 211
Varianten für den Abo-Status 211
Liste der Benachrichtigungen von Kaspersky Internet Security 213
Meldungen in allen Schutzmodi 213
Spezielle Desinfektionsprozedur ist erforderlich 214
Verstecktes Laden eines Treibers 214
Ein Programm ohne digitale Signatur wird gestartet 215
Ein Wechseldatenträger wurde angeschlossen 215
Neues Netzwerk wurde gefunden 215
Ein unsicheres Zertifikat wurde gefunden 216
Erlaubnisanfrage für den Zugriff auf eine Webseite aus einer regionalen Domain 216
Ein potentiell gefährliches Programm wurde gefunden 217
In Quarantäne befindliche Datei ist nicht infiziert 217
Eine neue Produktversion ist erschienen 218
Ein technisches Update ist erschienen 218
Ein technisches Update wurde heruntergeladen 218
Das heruntergeladene technische Update wurde nicht installiert 219
Lizenz abgelaufen 219
Meldungen im interaktiven Schutzmodus 220
Netzwerkaktivität eines Programms wurde erkannt 220
Verdächtiges Objekt wurde gefunden 221
Eine Schwachstelle wurde gefunden 222
Anfrage auf Erlaubnis für Programmaktionen 223
Gefährliche Aktivität im System wurde erkannt 223
Rollback von Änderungen, die von einem gefährlichen Programm ausgeführt wurden. 224

Ein schädliches Programm wurde gefunden 224
Ein verdächtiges Programm oder ein legales Programm, das von Angreifern verwendet werden kann, wurde gefunden 225
Ein verdächtiger / schädlicher Link wurde gefunden 226
Gefährliches Objekt wurde im Datenstrom gefunden 226
Ein versuchter Zugriff auf eine Phishing-Seite wurde erkannt 227
Versuch zum Zugriff auf die Systemregistrierung wurde erkannt 227
Desinfektion des Objekts ist nicht möglich 227
Versteckter Prozess wurde gefunden 228
Geo-Filter hat den Zugriff auf eine Webseite blockiert 229
Web-Filter hat den Download einer Webseite blockiert 229
Web-Filter hat den Download einer Webseite angehalten 230
Es wird empfohlen, in den Sicheren Browsermodus zu wechseln 230
Es wird empfohlen, den Sicheren Browsermodus zu verlassen 230
Bedienung des Programms über die Befehlszeile 231
Programm aktivieren 232
Programm starten 233
Programm beenden 233
Steuerung von Komponenten und Aufgaben des Programms 233
Virensuche 235
Programm-Update 237
Rollback zum vorherigen Update 238
Schutzparameter exportieren 238
Schutzparameter importieren 239
Protokolldatei anlegen 239
Hilfe anzeigen 240
Rückgabecodes der Befehlszeile 240
GLOSSAR 241
KASPERSKY LAB 251
INFORMATIONEN ZUM CODE VON DRITTHERSTELLERN 252
Programmcode 252
AGG 2.4 254
ADOBE ABI-SAFE CONTAINERS 1.0 255
BOOST 1.39.0 255
BZIP2/LIBBZIP2 1.0.5 255
CONVERTUTF 255
CURL 7.19.4 256
DEELX - REGULAR EXPRESSION ENGINE 1.2 256
EXPAT 1.2, 2.0.1 256
FASTSCRIPT 1.90 257
FDLIBM 5.3 257
FLEX: THE FAST LEXICAL ANALYZER 2.5.4 257
FMT.H 257
GDTOA 257
GECKO SDK 1.8, 1.9, 1.9.1 258
ICU4C 4.0.1 266
INFO-ZIP 5.51 266
JSON4LUA 0.9.30 267

LIBGD 2.0.35 267
LIBJPEG 6B 268
LIBM (lrint.c v 1.4, lrintf.c,v 1.5) 269
LIBPNG 1.2.8, 1.2.9, 1.2.42 270
LIBUNGIF 3.0 270
LIBXDR 270
LREXLIB 2.4 271
LUA 5.1.4 271
LZMALIB 4.43 272
MD5.H 272
MD5.H 272
MD5-CC 1.02 272
OPENSSL 0.9.8K 273
PCRE 7.7, 7.9 274
SHA1.C 1.2 276
STLPORT 5.2.1 276
SVCCTL.IDL 276
TINYXML 2.5.3 276
VISUAL STUDIO CRT SOURCE CODE 8.0 276
WINDOWS TEMPLATE LIBRARY 8.0 277
ZLIB 1.0.4, 1.0.8, 1.2.2, 1.2.3 281
Entwicklungstools 281
MS DDK 4.0, 2000 281
MS WDK 6000, 6001, 6002 281
WINDOWS INSTALLER XML (WIX) TOOLSET 3.0 281
Verteilter Programmcode 285
GRUB4DOS 0.4.4-2009-10-16 (FILE GRUB.EXE) 286
SYSLINUX 3.86 (FILE SYSLINUX.EXE) 290
Andere Informationen 294
SACHREGISTER 295

ENDNUTZER-LIZENZVERTRAG FÜR KASPERSKY LAB SOFTWARE

WICHTIGER RECHTLICHER HINWEIS AN ALLE NUTZER: LESEN SIE FOLGENDE RECHTLICHE VEREINBARUNG SORGFÄLTIG DURCH, BEVOR SIE DIE SOFTWARE NUTZEN.

INDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE AKZEPTIEREN KLICKEN ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEBEN, ERKLÄREN SIE SICH MIT DER EINHALTUNG DER GESCHÄFTSBEDINGUNGEN DIESES VERTRAGS EINVERSTANDEN. **DIESE AKTION KONSTITUIERT EIN BEKENNTNIS IHRER SIGNATUR UND SIE STIMMEN DIESER VEREINBARUNG, UND DASS SIE EINE PARTEI DIESER VEREINBARUNG WERDEN, ZU UND ERKLÄREN SICH WEITERHIN EINVERSTANDEN, DASS DIESE VEREINBARUNG, WIE JEDWEDE ANDERE SCHRIFTLICHE, AUSGEHANDELTE UND DURCH SIE UNTERZEICHNETE VEREINBARUNG AUCH, VOLLSTRECKBAR IST.** SOLLTEN SIE MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG NICHT EINVERSTANDEN SEIN, BEENDEN SIE DIE INSTALLATION DER SOFTWARE BZW. INSTALLIEREN SIE SIE NICHT.
NACHDEM SIE IM LIZENZVERTRAG-FENSTER AUF DIE SCHALTFLÄCHE AKZEPTIEREN GEKLICKT ODER EIN ENTSPRECHENDES ZEICHEN BZW. ENTSPRECHENDE ZEICHEN EINGEGEBEN HABEN, SIND SIE BERECHTIGT, DIE SOFTWARE IM EINKLANG MIT DEN GESCHÄFTSBEDINGUNGEN DIESER VEREINBARUNG ZU NUTZEN.

1. **Definitionen**
1.1. **Software** bezeichnet Software einschließlich aller Updates und zugehöriger Materialien.
1.2. **Rechtsinhaber** (Inhaber aller Rechte an der Software, ob exklusiv oder anderweitig) bezeichnet Kaspersky Lab ZAO, ein gemäß den Gesetzen der Russischen Föderation amtlich eingetragenes Unternehmen.
1.3. **Computer** bezeichnet/bezeichnen Hardware, einschließlich von PCs, Laptops, Workstations, PDAs, Smart Phones, tragbaren oder sonstigen elektronischen Geräten, für welche die Software konzipiert war und auf denen die Software installiert und/oder verwendet werden wird.
1.4. **Endnutzer (Sie)** bezeichnet eine bzw. mehrere Personen, die die Software in eigenem Namen installieren oder nutzen, oder die eine Software-Kopie rechtmäßig nutzt/nutzen, oder, falls die Software im Namen einer Organisation heruntergeladen oder installiert wurde, wie etwa einem Arbeitgeber, bezeichnet der Begriff *„Sie“* weiterhin jene Organisation, für die die Software heruntergeladen oder installiert wird, und es wird hiermit erklärt, dass eine solche Organisation die diese Vereinbarung akzeptierende Person autorisiert hat, dies in ihrem Namen zu tun. Im Sinne dieses Lizenzvertrags beinhaltet der Begriff *„Organisation“* ohne Einschränkungen jedwede Partnerschaft, GmbH, Gesellschaft, Vereinigung, Aktiengesellschaft, Treuhandgesellschaft, Gemeinschaftsunternehmen, Arbeitsorganisation, nicht eingetragene Organisation oder staatliche Behörde.
1.5. **Partner** bezeichnet Organisationen oder Personen, die die Software auf Grundlage eines Vertrags und einer mit dem Rechtsinhaber vereinbarten Lizenz vertreiben.
1.6. **Update(s)** bezeichnet/n alle Upgrades, Korrekturen, Patches, Erweiterungen, Reparaturen, Modifikationen, Kopien, Ergänzungen oder Wartungs-Softwarepakete usw.
1.7. **Benutzerhandbuch** bezeichnet die Bedienungsanleitung, die Administrator-Anleitung, ein Nachschlagewerk und ähnliche erläuternde oder sonstige Materialien.

2. Lizenzgewährung
2.1. Der Rechtsinhaber gewährt Ihnen hiermit eine nicht-ausschließliche Lizenz zur Speicherung, zum Laden, zur Installation, Ausführung und Darstellung (zur „Nutzung“) der Software auf einer festgelegten Anzahl von Computern zur Unterstützung des Schutzes Ihres Computers, auf dem die Software installiert ist, vor im Nutzerhandbuch beschriebenen Bedrohungen gemäß den technischen, im Benutzerhandbuch beschriebenen Anforderungen und im Einklang mit den Geschäftsbedingungen dieses Vertrags (die „Lizenz“). Sie erkennen diese Lizenz an.
Testversion. Sollten Sie eine Testversion der Software erhalten, heruntergeladen und/oder installiert haben und sollte Ihnen hiermit eine Evaluierungslizenz für die Software gewährt worden sein, dürfen Sie die Software ab dem Datum der ersten Installation nur zu Evaluierungszwecken verwenden, und zwar ausschließlich während der einzigen geltenden Evaluierungsperiode, außer wie anderweitig angegeben.

Jegliche Nutzung der Software zu anderen Zwecken oder über die geltende Evaluierungsperiode hinaus ist strikt untersagt.

Software für mehrere Umgebungen; Mehrsprachige Software; Dual-Medien-Software; Mehrere Kopien; Softwarebündel. Wenn Sie verschiedene Versionen der Software oder verschiedene Sprachausgaben der Software verwenden, wenn Sie die Software auf mehreren Medien erhalten, wenn Sie anderweitig mehrere Kopien der Software erhalten oder wenn Sie die Software mit einer anderen Software gebündelt erhalten sollten, entspricht die insgesamt zulässige Anzahl Ihrer Computer, auf denen alle Versionen der Software installiert sind, der Anzahl der Computer, die in den Lizenzen festgelegt ist, die Sie vom Rechtsinhaber bezogen haben, und jede erworbene Lizenz berechtigt Sie zur Installation und Nutzung der Software auf dieser Anzahl von Computern entsprechend den Festlegungen in den Klauseln 2.2 und 2.3, *außer die* Lizenzbedingungen sehen eine anderweitige Regelung vor.

2.2. Wenn die Software auf einem physischen Medium erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die auf der Softwareverpackung festgelegt ist.
2.3. Wenn die Software über das Internet erworben wurde, haben Sie das Recht, die Software zum Schutz einer solchen Anzahl von Computern zu verwenden, die genannt wurde, als Sie die Lizenz für die Software erworben haben.
2.4. Sie haben das Recht, eine Kopie der Software anzufertigen, und zwar ausschließlich zu Sicherungszwecken und nur, um die rechtmäßig in Ihrem Besitz befindliche Kopie zu ersetzen, sollte eine solche Kopie verloren gehen, zerstört oder unbrauchbar werden. Diese Sicherungskopie kann nicht zu anderen Zwecken verwendet werden und muss zerstört werden, wenn Sie das Recht verlieren, die Software zu nutzen oder wenn Ihre Lizenz abläuft oder aus irgendeinem Grund im Einklang mit der gültigen Gesetzgebung im Land Ihres Wohnsitzes oder in dem Land, in dem Sie die Software nutzen, gekündigt werden sollte.
2.5. Sie können die nicht-exklusive Lizenz zur Nutzung der Software an andere Personen innerhalb des Rahmens der Ihnen vom Rechtsinhaber gewährten Lizenz übertragen, vorausgesetzt, dass der Empfänger allen Geschäftsbedingungen dieses Vertrags zustimmt bzw. bejaht, Sie vollständig in der vom Rechtsinhaber gewährten Lizenz zu vertreten. In dem Fall, dass Sie die vom Rechtsinhaber gewährten Rechte zur Nutzung der Software vollständig übertragen, müssen Sie alle Kopien der Software, und zwar einschließlich der Sicherungskopie, zerstören. Wenn Sie Empfänger einer übertragenen Lizenz sind, müssen Sie zustimmen, alle Geschäftsbedingungen dieses Vertrags einzuhalten. Wenn Sie den Geschäftsbedingungen dieses Vertrags nicht vollständig zustimmen, dürfen Sie die Software nicht installieren und/oder verwenden. Sie stimmen als Empfänger einer übertragenen Lizenz weiterhin zu, dass Sie über keine zusätzlichen oder besseren Rechte verfügen, als der ursprüngliche Endnutzer, der die Software vom Rechtsinhaber erworben hat.
2.6 Ab dem Zeitpunkt der Aktivierung der Software bzw. Installation der Lizenzschlüsseldatei (mit Ausnahme einer Testversion der Software) haben Sie das Recht, folgende Dienstleistungen für den auf der Softwareverpackung (falls Sie Software auf einem physischen Medium erworben haben) oder während des Erwerbs (falls die Software über das Internet erworben wurde) festgelegten Zeitraum zu beziehen:
- Updates der Software über das Internet, wenn und wie der Rechtsinhaber diese auf seiner Webseite oder mittels anderer Online-Dienste veröffentlicht. Jedwede Updates, die Sie erhalten, werden Teil der Software und die Geschäftsbedingungen dieses Vertrags gelten für diese;
- Technische Unterstützung über das Internet sowie technische Unterstützung über die Telefon-Hotline.

3. Aktivierung und Zeitraum

3.1. Falls Sie Modifikationen an Ihrem Computer oder an der darauf installierten Software anderer Anbieter vornehmen, kann der Rechtsinhaber von Ihnen verlangen, die Aktivierung der Software bzw. die Installation der Lizenzschlüsseldatei zu wiederholen. Der Rechtsinhaber behält sich das Recht vor, jegliche Mittel und Verifizierungsverfahren zu nutzen, um die Gültigkeit der Lizenz und/oder die Rechtmäßigkeit einer Kopie der Software, die auf Ihrem Computer installiert und/oder genutzt wird, zu verifizieren.
3.2. Falls die Software auf einem physischen Medium erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags mit Beginn ab dem Zeitpunkt der Annahme dieses Vertrags für die auf der Verpackung bezeichnete Periode genutzt werden.
3.3. Falls die Software über das Internet erworben wurde, kann die Software nach Ihrer Annahme dieses Vertrags für die während des Erwerbs bezeichnete Zeitdauer genutzt werden.
3.4. Sie haben das Recht, eine Testversion der Software zu nutzen, und zwar gemäß der Festlegung in Klausel 2.1 und ohne jedwede Gebühr für die einzelne geltende Evaluierungsperiode (30 Tage) ab dem Zeitpunkt der Aktivierung der Software im Einklang mit diesem Vertrag, *und zwar unter der Bedingung, dass* die Testversion Ihnen nicht das Recht auf Updates und technische Unterstützung über das Internet und

technische Unterstützung über die Telefon-Hotline einräumt. Wenn der Rechtsinhaber für die einzelne geltende Evaluierungsperiode einen anderen Zeitraum festlegt, erhalten Sie darüber eine Mitteilung.
3.5. Ihre Lizenz zur Nutzung der Software beschränkt sich auf den in den Klauseln 3.2 oder 3.3 (je nach Anwendbarkeit) bezeichneten Zeitraum. Die verbleibende Zeitdauer kann auf die im Benutzerhandbuch beschriebene Weise abgefragt werden.
3.6. Haben Sie die Software zur Nutzung auf mehr als einem Computer erworben, beginnt der Zeitraum, auf den Ihre Lizenz zur Nutzung der Software begrenzt ist, am Tag der Aktivierung der Software bzw. der Installation der Lizenzschlüsseldatei auf dem ersten Computer.
3.7. Unbeschadet anderer Rechtsmittel laut Gesetz oder Billigkeitsrecht, zu denen der Rechtsinhaber im Falle eines Verstoßes gegen die Geschäftsbedingungen dieses Vertrags durch Sie berechtigt ist, ist der Rechtsinhaber jederzeit, ohne Sie benachrichtigen zu müssen, dazu berechtigt, diese Lizenz zur Nutzung der Software zu kündigen, und zwar ohne den Verkaufspreis oder einen Teil davon zurückzuerstatten.
3.8. Sie stimmen zu, dass Sie bei der Nutzung der Software sowie bei der Verwendung jedweder Berichte oder Informationen, die sich als Ergebnis der Nutzung der Software ableiten, alle geltenden internationalen, nationalen, staatlichen, regionalen und lokalen Gesetze sowie gesetzlichen Bestimmungen, einschließlich (und ohne Beschränkung) Datenschutz-, Urheber-, Exportkontroll- und Verfassungsrecht, einhalten werden.
3.9. Außer wenn anderweitig hierin festgelegt, dürfen Sie keines der Rechte, die Ihnen unter diesem Vertrag gewährt werden, bzw. keine Ihrer hieraus entstehenden Pflichten übertragen oder abtreten.
3.10. Der Rechtsinhaber behält sich das Recht vor, die Möglichkeit zur Aktivierung der Software außerhalb der Region, in der sie vom Rechtsinhaber und/oder seinen Partnern erworben wurde, zu beschränken.
3.11. Wenn Sie die Software mit einem Aktivierungscode erworben haben, der gültig für eine Sprachversion der Software in der Region ist, in der sie vom Rechtsinhaber oder seinen Partnern erworben wurde, dann können Sie die Software nicht durch Anwendung eines Aktivierungscodes aktivieren, der für eine andere Sprachversion vorgesehen ist.
3.12. Im Falle von Beschränkungen, die unter den Punkten 3.10 und 3.11 spezifiziert werden, wird die entsprechende Information über diese Beschränkungen auf der Verpackung und/oder Internetseite des Rechtsinhabers und/oder seiner Partner angegeben.

4. Technische Unterstützung
4.1. Die in Klausel 2.6 dieses Vertrags erläuterte technische Unterstützung wird Ihnen gewährt, wenn das neueste Update der Software installiert wird (außer im Fall einer Testversion der Software).
Technischer Support: http://support.kaspersky.com

5. Sammeln von Informationen
5.1. Durch Zustimmung zu den Geschäftsbedingungen dieses Vertrags haben Sie eingewilligt, dem Rechtsinhaber Informationen über die ausführbaren Dateien und ihre Prüfsummen zur Verfügung zu stellen, um Ihr Sicherheits-Schutzniveau zu verbessern.
5.2. Um das Sicherheitsbewusstsein bezüglich neuer Bedrohungen und deren Quellen zu verbessern, bzw. um Ihr Sicherheits-Schutzniveau zu verbessern, ist der Rechtsinhaber ausdrücklich berechtigt, mit Ihrer Zustimmung, die ausdrücklich in der Kaspersky Security Network Datenerfassungserklärung bestätigt wurde, derartige Informationen zu empfangen. Sie können den Kaspersky Security Network Service während der Installation deaktivieren. Sie können ebenfalls jederzeit auf der Softwareoptionsseite den Kaspersky Security Network Service aktivieren und deaktivieren.
Sie bestätigen und erkennen weiterhin an, dass jedwede Informationen, die vom Rechtsinhaber erfasst werden, zum Zweck der Verfolgung und Veröffentlichung von Sicherheitsrisikotrends verwendet werden können, und zwar nach freiem Ermessen des Rechtsinhabers.
5.3. Die Software verarbeitet keine personenbezogenen Daten und kombiniert keine Verarbeitungsdaten und persönlichen Informationen.
5.4. Sollten Sie nicht wünschen, dass die von der Software gesammelten Informationen an den Rechtsinhaber geschickt werden, sollten Sie den Kaspersky Security Network Service nicht aktivieren und/oder deaktivieren.

6. Beschränkungen
6.1. Sie werden die Software nicht emulieren, klonen, vermieten, verleihen, leasen, verkaufen, modifizieren, dekompilieren oder zurückentwickeln oder disassemblieren oder Arbeiten auf Grundlage der Software oder eines Teils davon ableiten, jedoch mit der einzigen Ausnahme eines Ihnen durch geltende Gesetzgebung gewährten Rechts, von dem keine Rücktretung möglich ist, und Sie werden in keiner anderen Form irgendeinen Teil der Software in menschlich lesbare Form umwandeln oder die lizenzierte Software oder irgendeine Teilmenge der lizenzierten Software übertragen, noch irgendeiner Drittpartei gestatten, dies zu tun, außer im Umfang vorangegangener Einschränkungen, die ausdrücklich durch geltendes Recht untersagt sind. Weder Binärcode noch Quellcode der Software dürfen verwendet oder zurückentwickelt

werden, um den Programmalgorithmus, der proprietär ist, wiederherzustellen. Alle Rechte, die nicht ausdrücklich hierin gewährt werden, verbleiben beim Rechtsinhaber und/oder dessen Zulieferern, je nachdem, was zutrifft. Jegliche derartige nicht autorisierte Nutzung der Software kann zur sofortigen und automatischen Kündigung dieses Vertrags sowie der hierunter gewährten Lizenz und zu Ihrer straf- und/oder zivilrechtlichen Verfolgung führen.
6.2. Sie werden die Rechte zur Nutzung der Software nicht an eine Drittpartei übertragen, außer entsprechend der Festlegung in Klausel 2.5 dieses Vertrags.
6.3. Sie werden den Aktivierungscode und/oder die Lizenzschlüssel-Datei keinen Drittparteien verfügbar machen oder Drittparteien Zugang zum Aktivierungscode und/oder zum Lizenzschlüssel gewähren. Aktivierungscode und/oder Lizenzschlüssel werden/wird als vertrauliche Daten des Rechtsinhabers betrachtet, und Sie werden angemessene Sorgfalt zum Schutz der Vertraulichkeit des Aktivierungscodes und/oder des Lizenzschlüssels walten lassen, sofern Sie den Aktivierungscode und/oder den Lizenzschlüssel entsprechend der Festlegung in Klausel 2.5 dieses Vertrags an Drittparteien übertragen dürfen.
6.4. Sie werden die Software nicht an eine Drittpartei vermieten, verleasen oder verleihen.
6.5. Sie werden die Software nicht zur Erstellung von Daten oder Software verwenden, die zur Feststellung, zum Sperren oder zur Handhabung von Bedrohungen, wie im Nutzerhandbuch beschrieben, genutzt werden.
6.6. Der Rechtsinhaber hat das Recht, die Schlüsseldatei zu blockieren oder Ihre Lizenz zu kündigen, falls Sie gegen irgendwelche Geschäftsbedingungen dieses Vertrags verstoßen, und zwar ohne irgendeine Rückerstattung an Sie.
6.7. Falls Sie die Testversion der Software verwenden, sind Sie nicht berechtigt, technische Unterstützung, wie in Klausel 4 dieses Vertrags festgelegt, zu erhalten, und Sie sind ebenfalls nicht berechtigt, die Lizenz oder die Rechte zur Nutzung der Software an irgendeine Drittpartei zu übertragen.

7. Eingeschränkte Garantie und Haftungsausschluss
7.1. Der Rechtsinhaber garantiert, dass die Software im Wesentlichen im Einklang mit den im Nutzerhandbuch dargelegten Spezifikationen und Beschreibungen funktionieren wird, *jedoch vorausgesetzt,* dass eine solche eingeschränkte Garantie nicht für Folgendes gilt: (w) Mängel Ihres Computers und zugehörigen Verstoß, wofür der Rechtsinhaber ausdrücklich jedwede Gewährleistungsverantwortung ablehnt; (x) Funktionsstörungen, Defekte oder Ausfälle, resultierend aus falscher Verwendung, Missbrauch, Unfall, Nachlässigkeit, unsachgemäßer/m Installation, Betrieb oder Wartung, Diebstahl, Vandalismus, höherer Gewalt, terroristischen Akten, Stromausfällen oder -schwankungen, Unglück, Veränderung, nicht zulässiger Modifikation oder Reparaturen durch eine Partei außer dem Rechtsinhaber oder Maßnahmen einer sonstigen Drittpartei oder Aktionen ihrerseits, oder Ursachen außerhalb der Kontrolle des Rechtsinhabers; (y) jedweder Defekt, der dem Rechtsinhaber nicht durch Sie bekannt gemacht wird, sobald dies nach dem ersten Auftreten des Defekts möglich ist; und (z) Inkompatibilität, verursacht durch Hardware- und/oder Software-Komponenten, die auf Ihrem Computer installiert sind.
7.2. Sie bestätigen, akzeptieren und erkennen an, dass keine Software frei von Fehlern ist, und Sie sind angehalten, den Computer mit einer für Sie geeigneten Häufigkeit und Beständigkeit zu sichern.
7.3. Der Rechtsinhaber gibt keine Garantie, dass die Software im Fall von Verstößen gegen die Bedingungen, wie im Nutzerhandbuch oder in diesem Vertrag beschrieben, einwandfrei funktionieren wird.
7.4. Der Rechtsinhaber garantiert nicht, dass die Software einwandfrei funktionieren wird, wenn Sie nicht regelmäßig, wie in Klausel 2.6 dieses Vertrags erläutert, Updates herunterladen.
7.5. Der Rechtsinhaber garantiert keinen Schutz vor im Nutzerhandbuch beschriebenen Bedrohungen nach Ablauf der in Klausel 3.2 oder 3.3 dieses Vertrags bezeichneten Periode oder nachdem die Lizenz zur Nutzung der Software aus irgendeinem Grund gekündigt wurde.
7.6. DIE SOFTWARE WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT UND DER RECHTSINHABER GIBT KEINE ZUSICHERUNG UND KEINE GEWÄHRLEISTUNG IN BEZUG AUF IHRE NUTZUNG ODER LEISTUNG. DER RECHTSINHABER UND SEINE PARTNER GEWÄHREN AUßER DEN GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN, DIE DURCH GELTENDES RECHT NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KÖNNEN, KEINE GARANTIEN, ZUSICHERUNGEN, BESTIMMUNGEN ODER BEDINGUNGEN (AUSDRÜCKLICHER ODER STILLSCHWEIGENDER NATUR, DIE ENTWEDER AUS EINER GESCHÄFTSBEZIEHUNG ODER EINEM HANDELSBRAUCH ENTSTEHEN BZW. AUS GESETZLICHEN, GEWOHNHEITSRECHTLICHTEN ODER ANDEREN VORSCHRIFTEN ABGELEITET WERDEN) HINSICHTLICH JEDWEDER ANGELEGENHEIT, EINSCHLIEßLICH (OHNE EINSCHRÄNKUNG) VON NICHTVERLETZUNG VON RECHTEN DRITTER, MARKTGÄNGIGKEIT, BEFRIEDIGENDE QUALITÄT, INTEGRIERUNG ODER BRAUCHBARKEIT FÜR EINEN BESTIMMTEN ZWECK. SIE TRAGEN DAS GESAMTE STÖRUNGSRISIKO UND DAS GESAMTRISIKO HINSICHTLICH DER LEISTUNG UND VERANTWORTUNG FÜR DIE AUSWAHL DER

SOFTWARE, UM IHRE VORGESEHENEN RESULTATE ZU ERZIELEN, UND FÜR DIE INSTALLATION SOWIE DIE NUTZUNG DER SOFTWARE UND DIE MIT IHR ERZIELTEN ERGEBNISSE. OHNE EINSCHRÄNKUNG DER VORANGEGANGENEN BESTIMMUNGEN MACHT DER RECHTSINHABER KEINE ZUSICHERUNGEN UND GIBT KEINE GEWÄHRLEISTUNG, DASS DIE SOFTWARE FEHLERFREI ODER FREI VON UNTERBRECHUNGEN ODER SONSTIGEN STÖRUNGEN IST ODER DASS DIE SOFTWARE JEDWEDE ODER ALL IHRE ANFORDERUNGEN ERFÜLLEN WIRD, UNGEACHTET DESSEN, OB GEGENÜBER DEM RECHTSINHABER OFFEN GELEGT ODER NICHT.

8. Haftungsausschluss und Haftungsbeschränkungen

8.1. INSOWEIT GESETZLICH STATTHAFT, SIND DER RECHTSINHABER UND SEINE PARTNER UNTER KEINEN UMSTÄNDEN HAFTBAR FÜR JEDWEDE SPEZIELLEN ODER BEILÄUFIGEN SCHÄDEN, STRAFZUSCHLAG ZUM SCHADENERSATZ, INDIREKTE ODER FOLGESCHÄDEN (EINSCHLIEßLICH UND NICHT BESCHRÄNKT AUF SCHÄDEN AUS VERLUST VON GEWINN ODER VERTRAULICHEN ODER SONSTIGEN INFORMATIONEN, FÜR GESCHÄFTSUNTERBRECHUNG, FÜR VERLUST VON PRIVATSPHÄRE, KORRUPTION, BESCHÄDIGUNG UND VERLUST VON DATEN ODER PROGRAMMEN, FÜR VERSÄUMNIS EINER PFLICHTERFÜLLUNG, EINSCHLIEßLICH JEDWEDER GESETZLICHER PFLICHTEN, TREUEPFLICHT ODER PFLICHT ZUR WAHRUNG ANGEMESSENER SORGFALT, FÜR NACHLÄSSIGKEIT, FÜR WIRTSCHAFTLICHEN VERLUST UND FÜR FINANZIELLEN ODER JEDWEDEN SONSTIGEN VERLUST), DIE AUS ODER AUF IRGENDEINE WEISE IM ZUSAMMENHANG MIT DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DER SOFTWARE, DER BEREITSTELLUNG ODER DEM VERSÄUMNIS DER BEREITSTELLUNG TECHNISCHER UNTERSTÜTZUNG ODER SONSTIGER DIENSTLEISTUNGEN, INFORMATIONEN, SOFTWARE UND ZUGEHÖRIGEM INHALT MITTELS DER SOFTWARE RESULTIEREN, ODER SICH ANDERWEITIG AUS DER NUTZUNG DER SOFTWARE ODER ANDERWEITIG UNTER BZW. IM ZUSAMMENHANG MIT EINER BESTIMMUNG DIESES VERTRAGS ERGEBEN, ODER DIE FOLGE EINES VERTRAGSBRUCHS ODER UNERLAUBTER HANDLUNG (EINSCHLIEßLICH NACHLÄSSIGKEIT, FALSCHANGABE, JEDWEDER STRIKTEN HAFTUNGSVERPFLICHTUNG ODER -PFLICHT), ODER EINER VERLETZUNG GESETZLICHER PFLICHTEN ODER DER GEWÄHRLEISTUNG DES RECHTSINHABERS ODER EINES SEINER PARTNER SIND, UND ZWAR AUCH DANN NICHT, WENN DER RECHTSINHABER ODER EINER SEINER PARTNER BEZÜGLICH DER MÖGLICHKEIT SOLCHER SCHÄDEN INFORMIERT WURDE.

SIE STIMMEN ZU, DASS IN DEM FALL, DASS DER RECHTSINHABER UND/ODER SEINE PARTNER HAFTBAR GEMACHT WERDEN/WIRD, DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER AUF DIE KOSTEN DER SOFTWARE BESCHRÄNKT IST. UNTER KEINEN UMSTÄNDEN WIRD DIE HAFTUNG DES RECHTSINHABERS UND/ODER SEINER PARTNER DIE FÜR DIE SOFTWARE ERSTATTETEN KOSTEN AN DEN RECHTSINHABER ODER DEN PARTNER ÜBERSTEIGEN (JE NACHDEM, WAS ZUTRIFFT).

NICHTS IN DIESEM VERTRAG SCHLIEßT EINEN ANSPRUCH AUFGRUND VON TOD UND PERSONENSCHADEN AUS ODER SCHRÄNKT DIESEN EIN. IN DEM FALL, DASS EIN HAFTUNGSAUSSCHLUSS, EIN AUSSCHLUSS ODER EINE EINSCHRÄNKUNG IN DIESEM VERTRAG AUFGRUND GELTENDEN RECHTS NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT WERDEN KANN, WIRD NUR EIN SOLCHER HAFTUNGSAUSSCHLUSS, AUSSCHLUSS ODER EINE EINSCHRÄNKUNG NICHT FÜR SIE GELTEN, UND SIE SIND WEITERHIN AN JEDWEDE VERBLEIBENDEN HAFTUNGSAUSSCHLÜSSE, AUSSCHLÜSSE ODER EINSCHRÄNKUNGEN GEBUNDEN.

9. GNU und sonstige Drittpartei-Lizenzen

9.1. Die Software kann einige Softwareprogramme enthalten, die an den Nutzer unter der GPL (GNU General Public License) oder sonstigen vergleichbaren freien Softwarelizenzen lizenziert (oder unterlizenziert) sind und dem Nutzer neben anderen Rechten gestatten, bestimmte Programme oder Teile dieser Programme zu kopieren, zu modifizieren und weiter zu verbreiten und sich Zugang zum Quellcode zu verschaffen („Open Source Software“). Falls es solche Lizenzen erforderlich machen, dass für jedwede Software, die an jemanden in ausführbarem Binärformat geliefert wird, diesen Nutzern der Quellcode ebenfalls verfügbar gemacht wird, dann soll der Quellcode zur Verfügung gestellt werden, indem ein diesbezügliches Ersuchen an source@kaspersky.com gesendet wird, oder der Quellcode wird mit der Software geliefert. Falls irgendwelche Open Source Software-Lizenzen es erforderlich machen, dass der Rechtsinhaber Rechte zur Nutzung, zum Kopieren oder zur Änderung eines Open Source Software-Programms bereitstellt, welche umfassender sind, als die in diesem Vertrag gewährten Rechte, dann werden derartige Rechte Vorrang vor den hierin festgelegten Rechten und Einschränkungen haben.

10. Geistiges Eigentum

10.1. Sie stimmen zu, dass die Software sowie die Urheberschaft, Systeme, Ideen, Betriebsmethoden, Dokumentation und sonstige in der Software enthaltenen Informationen proprietäres geistiges Eigentum und/oder die wertvollen Geschäftsgeheimnisse des Rechtsinhabers oder seiner Partner sind und dass der Rechtsinhaber und seine Partner, je nachdem was zutrifft, durch das Zivil- und Strafrecht sowie durch Gesetze zum Urheberrecht, bezüglich Geschäftsgeheimnissen, Handelsmarken und Patenten der Russischen Föderation, der Europäischen Union und der Vereinigten Staaten sowie anderer Länder und internationaler Übereinkommen geschützt sind. Dieser Vertrag gewährt Ihnen keinerlei Rechte am geistigen Eigentum, einschließlich an jeglichen Handelsmarken und Servicemarken des Rechtsinhabers und/oder seiner Partner („Handelsmarken“). Sie dürfen die Handelsmarken nur so weit nutzen, um von der Software im Einklang mit der akzeptierten Handelsmarkenpraxis erstellte Druckausgaben zu identifizieren, einschließlich der Identifizierung des Namens des Besitzers der Handelsmarke. Eine solche Nutzung der Handelsmarke gibt Ihnen keinerlei Besitzrechte an dieser Handelsmarke. Der Rechtsinhaber und/oder seine Partner besitzen und behalten alle Rechte, Titel und Anteile an der Software, einschließlich (ohne jedwede Einschränkung) jedweden Fehlerkorrekturen, Erweiterungen, Updates oder sonstigen Modifikationen an der Software, ob durch den Rechtsinhaber oder eine beliebige Drittpartei vorgenommen, und allen Urheberrechten, Patenten, Rechten an Geschäftsgeheimnissen, Handelsmarken und sonstigem geistigen Eigentum daran. Ihr Besitz, die Installation oder Nutzung der Software lässt den Titel am geistigen Eigentum an der Software nicht auf Sie übergehen, und Sie erwerben keinerlei Rechte an der Software, außer jene ausdrücklich in diesem Vertrag dargelegten. Alle hierunter erstellten Kopien der Software müssen dieselben proprietären Informationen enthalten, die auf und in der Software erscheinen. Mit Ausnahme der hierin aufgeführten Bestimmungen gewährt Ihnen dieser Vertrag keine Rechte geistigen Eigentums an der Software und Sie bestätigen, dass diese unter diesem Vertrag gewährte Lizenz Ihnen gemäß den weiteren Festlegungen hierin ausschließlich das Recht auf eingeschränkte Nutzung unter den Geschäftsbedingungen dieses Vertrags gewährt. Der Rechtsinhaber behält sich alle Rechte vor, die Ihnen nicht ausdrücklich in diesem Vertrag gewährt wurden.
10.2. Sie stimmen zu, die Software in keinster Weise zu modifizieren oder abzuändern. Sie dürfen die Urheberrechtshinweise oder sonstige proprietäre Hinweise auf jedweden Kopien der Software nicht entfernen oder verändern.

11. Geltendes Recht; Schiedsverfahren

11.1. Dieser Vertrag unterliegt den Gesetzen der Russischen Föderation und wird nach diesen ausgelegt, und zwar ohne Bezug auf gegenteilige gesetzliche Regelungen und Prinzipien. Dieser Vertrag wird nicht dem Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenverkauf unterliegen, dessen Anwendung ausschließlich ausgeschlossen wird. Jede Meinungsverschiedenheit, die aus den Bedingungen dieses Vertrags, deren Auslegung oder Anwendung oder einem Verstoß gegen diese resultiert, wird, außer falls durch unmittelbare Verhandlung beigelegt, durch das Gericht der internationalen Handelsschiedsgerichtsbarkeit bei der Industrie- und Handelskammer der Russischen Föderation in Moskau, in der Russischen Föderation, beigelegt. Jeder vom Schlichter abgegebene Schiedsspruch ist für die beteiligten Parteien endgültig und bindend und jedwedes Urteil bezüglich eines solchen Schiedsspruchs kann von jedem Gericht der zuständigen Jurisdiktion durchgesetzt werden. Nichts in diesem Abschnitt 11 wird eine Partei daran hindern, von einem Gericht der zuständigen Jurisdiktion rechtmäßige Entschädigung zu verlangen oder zu erhalten, sei es vor, während oder nach einem Schiedsverfahren.

12. Zeitraum für Rechtsverfolgung

12.1. Von den Parteien dieses Vertrags kann keine Rechtsverfolgung, ungeachtet der Form, die sich aus Transaktionen unter diesem Vertrag ergibt, nach mehr als einem (1) Jahr nach dem Eintreten des Klagegrundes oder der Entdeckung dessen Eintritts ergriffen werden, außer, dass eine Rechtsverfolgung für Verletzung von Rechten geistigen Eigentums innerhalb des maximal geltenden gesetzlichen Zeitraums ergriffen wird.

13. Vollständigkeit der Vereinbarung, Salvatorische Klausel, kein Verzicht

13.1. Dieser Vertrag stellt die Gesamtvereinbarung zwischen Ihnen und dem Rechtsinhaber dar und ersetzt jegliche sonstigen, vorherigen Vereinbarungen, Vorschläge, Kommunikation oder Ankündigung, ob mündlich oder schriftlich, in Bezug auf die Software oder den Gegenstand dieser Vereinbarung. Sie bestätigen, dass Sie diesen Vertrag gelesen haben, ihn verstehen und seinen Bedingungen zustimmen. Falls eine Bestimmung dieses Vertrags von einem Gericht der zuständigen Jurisdiktion insgesamt oder in Teilen als untauglich, ungültig oder aus welchen Gründen auch immer als nicht durchsetzbar angesehen wird, wird diese Bestimmung enger ausgelegt, damit sie rechtmäßig und durchsetzbar wird, und der Gesamtvertrag wird an diesem Umstand nicht scheitern, und die Ausgewogenheit des Vertrags bleibt weiterhin vollinhaltlich gültig und wirksam, so weit gesetzlich oder nach Billigkeitsrecht zulässig, während der ursprüngliche Inhalt

weitest möglich beibehalten wird. Kein Verzicht auf eine hierin enthaltene Bestimmung oder Kondition ist gültig, außer in schriftlicher Form und durch Sie und einen autorisierten Vertreter des Rechtsinhabers unterzeichnet, vorausgesetzt, dass kein Verzicht einer Verletzung einer Bestimmung dieses Vertrags einen Verzicht eines vorherigen, gleichzeitigen oder Folgeverstoßes konstituiert. Nichtverfolgung oder fehlende Durchsetzung einer Bestimmung dieses Vertrags durch den Rechtsinhaber kann nicht als Verzicht auf diese Bestimmung oder dieses Recht geltend gemacht werden.

14. Kontaktinformationen des Rechtsinhabers

Sollten Sie Fragen in Bezug auf diesen Vertrag haben oder sollten Sie wünschen, sich aus irgendeinem Grund mit dem Rechtsinhaber in Verbindung zu setzen, kontaktieren Sie bitte unsere Kundendienstabteilung unter:
Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
Moskau, 123060
Russische Föderation
Tel.: +7-495-797-8700
Fax: +7-495-645-7939
E-Mail: info@kaspersky.com
Webseite: http://www.kaspersky.com

© 1997-2010 Kaspersky Lab ZAO. Alle Rechte vorbehalten. Die Software und jedwede begleitende Dokumentation unterliegen dem Urheberrecht bzw. dem Schutz durch Urheberrechtsgesetze und internationale Urheberrechtsabkommen sowie durch weitere Gesetze und Abkommen zum geistigen Eigentum.

ÜBER DIESES HANDBUCH

Dieses Handbuch informiert über Installation, Konfiguration und Verwendung des Programms Kaspersky Internet Security 2011 (im Folgenden Kaspersky Internet Security genannt). Das Dokument ist für gewöhnliche Anwender gedacht. Zur Verwendung des Programms sind Grundkenntnisse im Umgang mit einem PC erforderlich: Der Anwender sollte das Interface und die Funktionen des Betriebssystems Microsoft Windows auf grundlegendem Niveau beherrschen sowie gängige E-Mail-Programme und Browser wie Microsoft Office Outlook und Microsoft Internet Explorer bedienen können.

Das Dokument soll:

- dem Anwender helfen, das Programm selbst auf einem Computer zu installieren, es zu aktivieren und unter Berücksichtigung individueller Aufgaben optimal anzupassen.
- Fragen, die sich auf das Programm beziehen, schnell beantworten.
- auf alternative Informationsquellen über das Programm und auf Möglichkeiten des technischen Supports hinweisen.

IN DIESEM ABSCHNITT

In diesem Dokument 19

Formatierung mit besonderer Bedeutung 20

IN DIESEM DOKUMENT

Dieses Dokument enthält folgende Abschnitte:

Zusätzliche Informationsquellen

Dieser Abschnitt enthält eine Beschreibung der Quellen, die zusätzliche Informationen über das Programm bieten, und verweist auf Internetressourcen, die zur Diskussion über das Programm, für Vorschläge, sowie für Fragen und Antworten dienen.

Kaspersky Internet Security 2011

Dieser Abschnitt enthält eine Beschreibung der Möglichkeiten der Anwendung und sowie über seine Komponenten und Grundfunktionen. Hier können Sie mehr über den Lieferumfang und die Services erfahren, die den registrierten Programmnutzern zur Verfügung stehen. Außerdem werden die Hard- und Softwarevoraussetzungen genannt, denen ein Computer entsprechen muss, damit Kaspersky Internet Security darauf installiert werden kann.

Programm installieren und deinstallieren

Dieser Abschnitt enthält Anleitungen, die dem Anwender helfen, das Programm auf einem Computer zu installieren oder eine Vorgängerversion zu aktualisieren. Dieser Abschnitt beschreibt, wie das Programm von einem Computer deinstalliert wird.

Lizenzverwaltung

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmlizenzierung zusammenhängen. In diesem Abschnitt erfahren Sie außerdem, wie die Gültigkeitsdauer für eine Lizenz automatisch verlängert werden kann und wo sich Informationen zur aktiven Lizenz befinden.

Programmoberfläche

Dieser Abschnitt beschreibt die wichtigsten Elemente der grafischen Programmoberfläche: Symbol und Kontextmenü des Programms, Hauptfenster, Konfigurationsfenster und Meldungsfenster.

Programm starten und beenden

Dieser Abschnitt informiert darüber, wie das Programm gestartet und beendet wird.

Schutzstatus des Computers

Dieser Abschnitt informiert darüber, wie ermittelt wird, ob der Computer im Augenblick sicher ist oder ob seine Sicherheit bedroht ist. Außerdem wird die Neutralisierung von vorhandenen Bedrohungen beschrieben. Hier finden Sie Informationen darüber, wie der Schutz während der Arbeit von Kaspersky Internet Security aktiviert, deaktiviert und vorübergehend angehalten werden kann.

Lösungen für typische Aufgaben

Dieser Abschnitt bietet eine Anleitung für die grundlegenden Augaben des Programms, die der Benutzer am häufigsten benötigt.

Erweiterte Programmeinstellungen

Dieser Abschnitt informiert ausführlich über die einzelnen Komponenten und beschreibt den jeweiligen Funktionsalgorithmus und die Einstellungen.

Überprüfung der Programmeinstellungen

Dieser Abschnitt enthält Tipps zur Überprüfung der Einstellungen für die Programmkomponenten.

Kontaktaufnahme mit dem Technischen Support

Dieser Abschnitt enthält Tipps dazu, wie Sie auf der Support-Webseite aus Mein Kaspersky Account oder telefonisch Hilfe von Kaspersky Lab erhalten können.

Anhänge

Dieser Abschnitt enthält Hilfeinformationen, die den Haupttext des Dokuments ergänzen.

Glossar

Dieser Abschnitt enthält eine Liste und Definitionen der Begriffe, die in diesem Dokument vorkommen.

FORMATIERUNG MIT BESONDERER BEDEUTUNG

Die Bedeutung der in diesem Dokument verwendeten Textformatierungen wird in folgender Tabelle erläutert.

Tabelle 1. Formatierung mit besonderer Bedeutung

TEXTBEISPIEL	BESCHREIBUNG DER FORMATIERUNG
Beachten Sie, dass ...	Warnungen sind rot geschrieben und eingerahmt. Warnungen enthalten wichtige Informationen, die z.B. auf Aktionen hinweisen, die im Hinblick auf die Computersicherheit als kritisch gelten.

TEXTBEISPIEL	BESCHREIBUNG DER FORMATIERUNG
Es wird empfohlen,...	Hinweise sind eingerahmt. Hinweise enthalten hilfreiche und informative Angaben.
Beispiel: ...	Beispiele sind gelb unterlegt und mit "Beispiel" überschrieben.
Das *Update* ist...	Neue Begriffe sind kursiv geschrieben.
ALT+F4	Bezeichnungen von Tasten sind halbfett und in Großbuchstaben geschrieben. Tastenbezeichnungen, die mit einem Pluszeichen verbunden sind, bedeuten eine Tastenkombination.
Aktivieren	Die Namen von Elementen der Benutzeroberfläche (z.B. Eingabefelder, Menübefehle, Schaltflächen) sind halbfett geschrieben.
Gehen Sie folgendermaßen vor, um den Aufgabenzeitplan anzupassen:	Der erste Satz einer Anleitung ist kursiv geschrieben.
`help`	Texte in der Befehlszeile oder Meldungstexte, die das Programm auf dem Bildschirm anzeigt, werden durch spezielle Schrift hervorgehoben.
<IP-Adresse Ihres Computers>	Variable stehen in eckigen Klammern. Eine Variable muss in einem konkreten Fall durch einen entsprechenden Wert ersetzt werden. Dabei fallen die eckigen Klammern weg.

ZUSÄTZLICHE INFORMATIONSQUELLEN

Fragen zu Auswahl, Kauf, Installation oder Verwendung von Kaspersky Internet Security haben, lassen sich unter Verwendung unterschiedlicher Informationsquellen beantworten. Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage eine passende Quelle wählen.

IN DIESEM ABSCHNITT

Informationsquellen zur selbständigen Recherche 22

Diskussion über die Programme von Kaspersky Lab im Webforum 23

Kontaktaufnahme mit der Vertriebsabteilung 23

Kontakt zur Abteilung für Handbücher und Hilfesysteme 23

INFORMATIONSQUELLEN ZUR SELBSTÄNDIGEN RECHERCHE

Kaspersky Lab bietet folgende Informationsquellen zu dem Programm an:

- Seite über das Programm auf der Webseite von Kaspersky Lab
- Seite über das Programm auf der Webseite des Technischen Supports (in der Wissensdatenbank)
- Seite des Interaktiven Supports
- Elektronisches Hilfesystem

Seite auf der Webseite von Kaspersky Lab

Auf dieser Seite (http://www.kaspersky.de/kaspersky_internet_security) finden Sie allgemeine Informationen über das Programm, seine Funktionen und Besonderheiten.

Seite auf der Webseite des Technischen Supports (Wissensdatenbank)

Auf dieser Seite (http://support.kaspersky.de/kis2011) finden Sie Artikel, die von Spezialisten des technischen Supports veröffentlicht wurden.

Diese Artikel bieten nützliche Informationen, Tipps und Antworten auf häufige Fragen zu Kauf, Installation und Verwendung vom Programm. Sie sind nach Themen wie "Mit der Produktlizenz arbeiten", "Update anpassen" oder "Störungen bei der Arbeit beheben" angeordnet. Die Artikel können auch Fragen behandeln, die neben diesem Programm auch andere Produkte von Kaspersky Lab betreffen. Außerdem können sie allgemeine Neuigkeiten über den Technischen Support enthalten.

Interaktiver Support

Auf der Seite dieses Dienstes finden Sie eine regelmäßig aktualisierte Datenbank mit häufig auftretenden Fragen und Antworten über die Arbeit des Programms. Um diesen Dienst nutzen zu können, ist eine Internetverbindung erforderlich.

Um zur Serviceseite zu wechseln, verwenden Sie im Programmhauptfenster den Link **Support** und klicken Sie im folgenden Fenster auf **Interaktiver Support**.

Elektronisches Hilfesystem

Im Lieferumfang des Programms ist eine vollständige und kontextorientierte Hilfedatei enthalten. Sie bietet Informationen zu folgenden Aspekten des Computerschutzes: Anzeige des Schutzstatus, Untersuchung bestimmter Computerbereiche auf Viren, Ausführen anderer Aufgaben. Außerdem bietet die vollständige kontextorientierte Hilfe Informationen zu jedem Programmfenster: Liste und Beschreibung der darin enthaltenen Einstellungen und Liste der entsprechenden Aufgaben.

Um die Hilfe zu öffnen, klicken Sie im entsprechenden Fenster auf **Hilfe** oder auf die Taste **F1**.

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM WEBFORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum unter der Adresse http://www.kaspersky.de/forum diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben, neue Themen eröffnen und die Hilfefunktion verwenden.

KONTAKTAUFNAHME MIT DER VERTRIEBSABTEILUNG

Bei Fragen zur Auswahl oder zum Kauf von der Kaspersky Produkte sowie zur Verlängerung der Nutzungsdauer stehen Ihnen die Mitarbeiter der Vertriebsabteilung in Deutschland unter folgenden Rufnummern zur Verfügung:

+49 (0) 841 – 981 89 560

Die Beratung erfolgt auf Deutsch oder Englisch.

Sie können sich mit Ihrer Frage auch über unser Kontaktformular an die Mitarbeiter der Vertriebsabteilung wenden.

KONTAKT ZUR ABTEILUNG FÜR HANDBÜCHER UND HILFESYSTEME

Wenn Sie Fragen zu dieser Dokumentation haben, einen Fehler darin gefunden haben oder Ihre Meinung über unsere Dokumentationen schreiben möchten, richten Sie sich bitte direkt an unsere Abteilung für Handbücher und Hilfesysteme. Um Kontakt mit der Abteilung für Handbücher und Hilfesysteme aufzunehmen, schreiben Sie an docfeedback@kaspersky.com. Geben Sie folgenden Betreff an: "Kaspersky Help Feedback: Kaspersky Internet Security".

KASPERSKY INTERNET SECURITY 2011

Dieser Abschnitt enthält eine Beschreibung der Möglichkeiten der Anwendung und sowie über seine Komponenten und Grundfunktionen. Hier können Sie mehr über den Lieferumfang und die Services erfahren, die den registrierten Programmnutzern zur Verfügung stehen. Außerdem werden die Hard- und Softwarevoraussetzungen genannt, denen ein Computer entsprechen muss, damit Kaspersky Internet Security darauf installiert werden kann.

IN DIESEM ABSCHNITT

Neuerungen 24

Organisation des Schutzes für Ihren Computer 25

Lieferumfang 27

Service für registrierte Benutzer 27

Hard- und Softwarevoraussetzungen 28

NEUERUNGEN

Kaspersky Internet Security verfügt über folgende Neuerungen:

- Die neue Schutzkomponente Netzwerkmonitor (s. S. 121) verfolgt die Aktivität von Programmen im System und versorgt andere Schutzkomponenten mit Zusatzinformationen. Die Speicherung eines Aktivitätsverlaufs der Programme erlaubt es der Komponente, die Aktionen eines Schadprogramms rückgängig zu machen, wenn bestimmte Schutzkomponenten eine schädliche Aktivität erkennen.

- Die sichere Umgebung enthält mit *Sicherer Programmstart* (s. S. 164) einen isolierten Desktop, auf dem Sie verdächtige Programme starten können, ohne dass das normale Betriebssystem gefährdet wird.

- Der Schutz für die Arbeit im Internet wurde durch folgende neue Module verbessert:

  - Web-Filter (s. S. 115) umfasst ein Modul zur Link-Untersuchung, das bereits aus der Vorgängerversion des Programms bekannt ist, und bietet außerdem die Möglichkeit, den Zugriff auf riskante Seiten zu blockieren. Auf diese Weise befinden Sie sich stets in einer sicheren Internetzone.

  - Geo-Filter (s. S. 115) erlaubt Ihnen, den Zugriff auf Seiten aufgrund ihrer Zugehörigkeit zu Domains zu erlauben oder zu verbieten. Dadurch lässt sich beispielsweise der Zugriff auf Webseiten verbieten, die regionalen Domains mit einem hohem Kontaminationsgrad angehören.

- Die Programmkontrolle bietet eine verbesserte Statusermittlung für Programme und eine effektivere Konfiguration von Programmregeln. Dabei werden Daten aus Kaspersky Security Network verwendet, denen eine Statistik über die Arbeit der Programmkontrolle auf einer großen Anzahl von PCs zugrundeliegen.

- Mit Hilfe der Untersuchung im Computerleerlauf (s. S. 183) kann eine Virenuntersuchung des Computers jetzt in Zeiträumen ausgeführt werden, in denen Sie nicht mit dem Computer arbeiten, und die Suche wird abgebrochen, wenn Sie wieder an den Computer zurückkehren. Dadurch wird erlaubt, regelmäßig eine Untersuchung des Computers auszuführen und die Performance des Computers nicht zu beeinträchtigen, während Sie den Computer benötigen.

- Die Funktionalität der Kindersicherung (s. S. 169) wurde erweitert. Es stehen folgende Optionen für einen Benutzer zur Verfügung: Kontrolle des Zugriffs auf den Computer und auf das Internet, Kontrolle über den Start von Computerprogrammen, Beschränkung der Anzeige von Webseiten mit unerwünschtem Inhalt und Beschränkung des Datei-Downloads aus dem Internet, Kontrolle der Kommunikation eines Benutzers in sozialen Netzwerken und mit Instant Messenger, Anzeige von Berichten über die Aktionen eines kontrollierten

Benutzers. Um die Konfiguration der Kindersicherung zu optimieren, sind Export und Import von Funktionsparametern der Komponente für ein Benutzerkonto vorgesehen.

- Wenn Kaspersky Internet Security auf einem Computer mit dem Betriebssystem Microsoft Windows Vista oder Microsoft Windows 7 eingesetzt wird, steht das Kaspersky Gadget zur Verfügung (weiter auch einfach als *Gadget* bezeichnet). Kaspersky Gadget bietet schnellen Zugriff auf die Grundfunktionen des Programms: Schutzstatus des Computers anzeigen, Objekte auf Viren untersuchen, Berichte über die Programmarbeit anzeigen, u.a.

ORGANISATION DES SCHUTZES FÜR IHREN COMPUTER

Kaspersky Internet Security bietet Ihrem Computer einen komplexen Schutz vor bekannten und neuen Bedrohungen, Netzwerkangriffen und Betrugsversuchen, Spam und anderen unerwünschten Informationen.

Jeder Bedrohungstyp wird von einer speziellen *Schutzkomponente* verarbeitet (s. Beschreibung der Komponenten weiter unten in diesem Abschnitt). Die Komponenten können unabhängig voneinander aktiviert und deaktiviert werden und lassen sich flexibel anpassen.

Zusätzlich zum Echtzeitschutz, den die Schutzkomponenten realisieren, wird eine regelmäßige *Untersuchung* Ihres Computers empfohlen. Das ist erforderlich, um die Möglichkeit der Ausbreitung schädlicher Programme auszuschließen, die nicht von den Schutzkomponenten erkannt wurden, weil beispielsweise eine zu niedrige Schutzstufe eingestellt war.

Um Kaspersky Internet Security auf dem neuesten Stand zu halten, ist ein *Update* der Datenbanken und Programm-Module erforderlich, die bei der Arbeit des Programms verwendet werden. Das Programm wird in der Grundeinstellung automatisch aktualisiert. Bei Bedarf können Datenbanken und Programm-Module aber jederzeit auf Befehl aktualisiert werden.

Der Start bestimmter Programmen, die auf Ihrem Computer installiert sind, kann kontrolliert werden. Dazu dient die *Aktivitätskontrolle für Programme*. Der Zugriff von Programmen auf *persönliche Daten* wird auf spezielle Art kontrolliert. Zu diesen Daten zählen Dateien, Ordner und Registrierungsschlüssel, die Funktionsparameter und wichtige Daten für häufig verwendete Programme enthalten, sowie Dateien des Benutzers (Ordner Eigene Dateien, Cookie-Dateien, Daten über die Benutzeraktivität). Programme, an deren Sicherheit Sie zweifeln, können in der speziellen *Sicheren Umgebung* gestartet werden.

Einige spezifische Aufgaben, die nicht regelmäßig, sondern nur gelegentlich anfallen, werden mit Hilfe zusätzlicher Tools und Assistenten ausgeführt (s. Abschnitt "Zusätzliche Schutz-Tools" auf S. 188). Dazu zählen beispielsweise die Konfiguration des Browsers Microsoft Internet Explorer oder das Löschen von Aktivitätsspuren des Benutzers im System.

Schutzkomponenten

Der Echtzeitschutz Ihres Computers wird durch folgende Komponenten gewährleistet.

Datei-Anti-Virus

Datei-Anti-Virus schützt das Dateisystem des Computers vor einer Infektion. Die Komponente wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die auf Ihrem Computer und auf allen angeschlossenen Laufwerken geöffnet, gespeichert und gestartet werden. Kaspersky Internet Security fängt jeden Zugriff auf eine Datei ab und untersucht die Datei nach bekannten Viren. Eine Datei wird nur dann zur Arbeit freigegeben, wenn die Datei virenfrei ist oder erfolgreich vom Programm desinfiziert wurde. Wenn die Desinfektion einer Datei nicht möglich ist, wird sie gelöscht. Dabei wird eine Kopie der Datei im Backup abgelegt oder in der Quarantäne gespeichert.

Mail-Anti-Virus

Mail-Anti-Virus untersucht ein- und ausgehende E-Mails auf Ihrem Computer. Eine E-Mail wird nur dann dem Empfänger zugestellt, wenn sie keine gefährlichen Objekte enthält.

Web-Anti-Virus

Web-Anti-Virus fängt die Ausführung von Skripts, die sich auf Webseiten befinden, ab und blockiert sie, falls Sie gefährlich sind. Auch der Web-Datenverkehr unterliegt einer strengen Kontrolle. Außerdem blockiert die Komponente den Zugriff auf gefährliche Webseiten.

IM-Anti-Virus

IM-Anti-Virus sorgt für die Sicherheit bei Instant Messengern. Die Komponente schützt die Informationen, die über Instant Messenger-Protokolle auf Ihren Computer gelangen. IM-Anti-Virus gewährleistet Sicherheit bei der Arbeit mit vielen Programmen, die dem Sofortaustausch von Nachrichten dienen.

Proaktiver Schutz

Der Proaktive Schutz erlaubt es, ein neues Schadprogramm zu erkennen, bevor es Schaden anrichten kann. Die Arbeit der Komponente basiert auf der Kontrolle und Analyse des Verhaltens aller auf Ihrem Computer installierten Programme. Abhängig von den auszuführenden Aktionen entscheidet Kaspersky Internet Security, ob ein Programm potentiell gefährlich ist. So ist Ihr Computer nicht nur vor bekannten Viren, sondern auch vor neuen, bisher unbekannten Viren geschützt.

Anti-Phishing

Komponente, die in Web-Anti-Virus, Anti-Spam und IM-Anti-Virus integriert ist und mit der Webadressen auf ihre Zugehörigkeit zur Liste der Phishing- und verdächtigen Webadressen untersucht werden können.

Programmkontrolle

Programmkontrolle registriert die Aktionen, die von Programmen im System ausgeführt werden können, und reguliert in Abhängigkeit von der Gruppe, zu der ein Programm gehört, seine Aktivität. Für jede Gruppe von Programmen ist eine Auswahl von Regeln vorgegeben. Diese Regeln steuern den Zugriff von Programmen auf unterschiedliche Ressourcen des Betriebssystems.

Firewall

Firewall gewährleistet Sicherheit bei der in lokalen Netzwerken und im Internet. Die Komponente führt die Filterung der gesamten Netzwerkaktivität durch, wozu zwei Arten von Regeln dienen: *Regeln für Programme* und *Paketregeln*.

Schutz vor Netzwerkangriffen

Der Schutz vor Netzwerkangriffen wird beim Hochfahren des Betriebssystems gestartet und überwacht den eingehenden Datenverkehr auf für Netzwerkangriffe charakteristische Aktivität. Wenn ein Angriffsversuch auf Ihren Computer erkannt wird, blockiert Kaspersky Internet Security jede Art von Netzwerkaktivität des angreifenden Computers im Hinblick auf Ihren Computer.

Anti-Spam

Anti-Spam wird in Ihr Mailprogramm integriert und kontrolliert alle eingehenden E-Mail auf Spam. Alle E-Mails, die Spam enthalten, werden durch eine spezielle Kopfzeile markiert. Anti-Spam kann zusätzlich für die Spam-Verarbeitung (automatisches Löschen, Verschieben in einen speziellen Ordner, u.a.) eingestellt werden. Außerdem analysiert die Komponente E-Mails im Hinblick auf Phishing.

Netzwerkmonitor

Diese Komponente dient dazu, in Echtzeit Informationen über die Netzwerkaktivität anzuzeigen.

Anti-Banner

Anti-Banner blockiert Werbung, die auf speziellen Bannern platziert ist, die in das Interface von auf Ihrem Computer installierten Programmen integriert sind oder sich im Internet befinden.

Kindersicherung

Die Funktionen der Kindersicherung dienen dazu, Kinder und Jugendliche vor Gefahren zu schützen, die bei der Arbeit am Computer und im Internet bestehen.

Die Kindersicherung erlaubt es, den Zugriff auf Internetressourcen und Programme für unterschiedliche Computerbenutzer altersabhängig flexibel einzuschränken. Außerdem erlaubt es diese Funktion, Berichte mit einer Statistik über die Aktionen der kontrollierten Benutzer anzuzeigen:

Es werden drei Gruppen von Objekten unterschieden, an deren Schutz die Programmkomponenten beteiligt sind:

- Dateien, persönliche Daten, Benutzernamen und Kennwörter, Daten über Scheckkarten usw. Am Schutz dieser Objekte sind Datei-Anti-Virus, Programmkontrolle und Proaktiver Schutz beteiligt.
- Auf Ihrem Computer installierte Programme und Objekte des Betriebssystems. Am Schutz dieser Objekte sind Mail-Anti-Virus, Web-Anti-Virus, IM-Anti-Virus, Programmkontrolle, Schutz vor Netzwerkangriffen, Anti-Spam und Proaktiver Schutz beteiligt.
- Arbeit im Netzwerk: Anzeigen von Webseiten, Verwendung von Zahlungssystemen, Schutz des Posteingangs vor Spam und Viren usw. Am Schutz dieser Objekte sind Mail-Anti-Virus, Web-Anti-Virus, IM-Anti-Virus, Firewall, Schutz vor Netzwerkangriffen, Anti-Spam, Netzwerkmonitor, Anti-Banner und Kindersicherung beteiligt.

Eine Übersicht der Komponenten und der von ihnen geschützten Objekte befindet sich im Abschnitt **Schutz-Center** des Programmhauptfensters (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47).

LIEFERUMFANG

Sie können Kaspersky Internet Security bei unseren Vertriebspartnern (CD-Box) sowie im Online-Shop kaufen (zum Beispiel http://www.kaspersky.de, Abschnitt **Online-Shop**).

Wurde das Programm in einer CD-Box erworben, gehören zum Lieferumfang des Programms:

- versiegelter Umschlag mit Installations-CD, auf der die Programmdateien und die Dokumentation im PDF-Format gespeichert sind.
- Kurzes Benutzerhandbuch, das einen Aktivierungscode enthält.
- Lizenzvertrag (je nach Region).

Lesen Sie sich den Lizenzvertrag (s. Abschnitt "Über den Lizenzvertrag" auf S. 42) genau durch!

Wenn Sie Kaspersky Internet Security in einem Online-Shop kaufen, kopieren Sie das Produkt von der Kaspersky-Lab-Webseite. Die Distribution enthält neben dem eigentlichen Produkt auch das vorliegende Handbuch. Ein Aktivierungscode wird Ihnen nach Eingang des Rechnungsbetrags per E-Mail zugestellt.

SERVICE FÜR REGISTRIERTE BENUTZER

Kaspersky Lab ZAO bietet den legalen Benutzern ein umfangreiches Spektrum an Leistungen an, die den wirkungsvollen Einsatz des Programms effektiver gestalten.

Durch den Kauf einer Lizenz werden Sie zum registrierten Benutzer und können während der Gültigkeitsdauer der Lizenz folgende Leistungen in Anspruch nehmen:

- Stündliches Update der Programm-Datenbanken und Upgrade auf neue Programmversionen.
- Beratung bei Fragen zur Installation, Konfiguration und Nutzung des Programms per Telefon und über Mein Kaspersky Account.
- Benachrichtigung über das Erscheinen neuer Kaspersky-Lab-Programme und über neue Viren. Dieser Service wird Benutzern geboten, die den Newsletter von Kaspersky Lab auf (http://www.kaspersky.de/lab-news) abonniert haben.

Die Beratung bezieht sich nicht auf Fragen zu Funktion und Gebrauch von Betriebssystemen, Software von Drittherstellern und Funktionsweise verschiedener Technologien.

HARD- UND SOFTWAREVORAUSSETZUNGEN

Um die normale Funktionsfähigkeit von Kaspersky Internet Security zu gewährleisten, sind folgende Systemvoraussetzungen zu erfüllen:

Allgemeine Anforderungen:

- 480 MB freier Speicherplatz auf der Festplatte
- CD / DVD-ROM-Laufwerk (für Installation von Kaspersky Internet Security von Installations-CD)
- Internetverbindung (für das Update von Datenbanken und Programm-Modulen)
- Microsoft Internet Explorer 6.0 oder höher
- Microsoft Windows Installer 2.0

Anforderungen für die Betriebssysteme Microsoft Windows XP Home Edition (Service Pack 2 oder höher), Microsoft Windows XP Professional (Service Pack 2 oder höher), Microsoft Windows XP Professional x64 Edition (Service Pack 2 oder höher):

- Prozessor Intel Pentium 800 MHz 32-Bit (x86)/ 64-Bit (x64) oder höher (oder ein entsprechender kompatibler Prozessor)
- 512 MB Arbeitsspeicher

Anforderungen für die Betriebssysteme Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate, Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:

- Prozessor Intel Pentium 1 GHz 32-Bit (x86)/ 64-Bit (x64) oder höher (oder ein entsprechender kompatibler Prozessor
- 1 GB Arbeitsspeicher (32-Bit); 2 GB Arbeitsspeicher (64-Bit)

Unter dem Betriebssystem Microsoft Windows XP (64-bit) ist die Verwendung der Sicheren Umgebung nicht möglich. Unter den Betriebssystemen Microsoft Windows Vista (64-bit) und Microsoft Windows 7(64-bit) ist die Verwendung der Sicheren Umgebung eingeschränkt.

Anforderungen für Netbooks:

- Prozessor Intel Atom 1.33 MHz (Z520) oder kompatibel.
- Grafikkarte Intel GMA950 mit Videospeicher von mindestens 64 MB (oder kompatibel).
- Bildschirmdiagonale mindestens 10.1 Zoll

PROGRAMM INSTALLIEREN UND DEINSTALLIEREN

Dieser Abschnitt enthält Anleitungen, die dem Anwender helfen, das Programm auf einem Computer zu installieren oder eine Vorgängerversion zu aktualisieren. Dieser Abschnitt beschreibt, wie das Programm von einem Computer deinstalliert wird.

IN DIESEM ABSCHNITT

Standard-Installationsmethode 29

Aktualisierung einer Vorgängerversion von Kaspersky Internet Security 34

Untypische Installationsszenarien 39

Erste Schritte 40

Programm deinstallieren 40

STANDARD-INSTALLATIONSMETHODE

Kaspersky Internet Security wird auf dem Computer interaktiv mit einem Installationsassistenten installiert.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Wird das Programm für den Schutz von mehr als einem Computer verwendet, so geht die Installation auf allen Computern identisch vor sich. Hierbei ist zu beachten, dass die Gültigkeitsdauer der Lizenz gemäß Lizenzvereinbarung mit der ersten Aktivierung des Programms beginnt.

- *Zur Installation von Kaspersky Internet Security auf Ihrem Computer,*

  starten Sie auf der Produkt-CD die Installationsdatei (Datei mit der Erweiterung .exe).

Der Installationsvorgang für das Programm Kaspersky Internet Security, das aus dem Internet bezogen wurde, ist identisch mit dem Installationsvorgang von der CD-ROM.

IN DIESEM ABSCHNITT

Schritt 1. Nach neuer Programmversion suchen 30

Schritt 2. Systemkompatibilität für Installation prüfen 30

Schritt 3. Installationstyp wählen 31

Schritt 4. Lizenzvereinbarung anzeigen 31

Schritt 5. Erklärung zur Verwendung von Kaspersky Security Network 31

Schritt 6. Inkompatible Programme suchen 31

Schritt 7. Installationsverzeichnis wählen 32

Schritt 8. Installation vorbereiten 32

Schritt 9. Installation 33

Schritt 10. Programm aktivieren 33

Schritt 11. Anmeldung des Benutzers 34

Schritt 12. Aktivierung abschließen 34

Schritt 13. Systemanalyse 34

Schritt 14. Assistent abschließen 34

SCHRITT 1. NACH NEUER PROGRAMMVERSION SUCHEN

Vor der Installation wird geprüft, ob neuere Versionen von Kaspersky Internet Security auf den Updateservern von Kaspersky Lab vorhanden sind.

Wenn keine neuere Version des Programms auf den Updateservern von Kaspersky Lab gefunden wurde, wird der Installationsassistent für diese Version gestartet.

Wenn auf den Updateservern eine neuere Version von Kaspersky Internet Security vorgefunden wurde, werden Ihnen Download und Installation vorgeschlagen. Es wird empfohlen, die neue Programmversion zu installieren, da neue Versionen den Schutz Ihres Computers optimieren. Sollten Sie die neuere Version ablehnen, wird der Installationsassistent der laufenden Version gestartet. Sollten Sie die Installation der neueren Version annehmen, werden die Programmdateien auf Ihren Computer kopiert und der Installationsassistent wird automatisch gestartet. Eine weitere Beschreibung zur Installation einer neueren Version finden Sie in der Dokumentation zur entsprechenden Programmversion.

SCHRITT 2. SYSTEMKOMPATIBILITÄT FÜR INSTALLATION PRÜFEN

Vor der Installation von Kaspersky Internet Security auf Ihrem Computer wird die Kompatibilität des Betriebssystems und der Service Packs mit den Softwarevoraussetzungen für die Installation abgeglichen Softwarevoraussetzungen für die Installation (s. Abschnitt "Hard- und Softwarevoraussetzungen" auf S. 28). Außerdem werden die Hardwarevoraussetzungen geprüft sowie die Rechte für die Installation des Programms. Wenn eine der aufgezählten Bedingung nicht erfüllt wird, erscheint eine entsprechende Meldung auf dem Bildschirm.

Wenn der Computer die Voraussetzungen erfüllt, sucht der Assistent nach Kaspersky-Lab-Programmen, deren gleichzeitige Verwendung mit Kaspersky Internet Security zu Konflikten führen kann. Wenn solche Programme gefunden werden, werden Sie aufgefordert, die Programme manuell zu entfernen.

Wenn sich unter den gefundenen Programmen eine Vorgängerversion von Kaspersky Anti-Virus oder Kaspersky Internet Security befindet, werden alle Daten, die von Kaspersky Internet Security 2011 verwendet werden können (Aktivierungsdaten, Programmeinstellungen usw.), gespeichert und das bereits installierte Programm wird automatisch gelöscht.

SCHRITT 3. INSTALLATIONSTYP WÄHLEN

In dieser Phase der Installation können Sie einen passenden Typ für die Installation von Kaspersky Internet Security auswählen:

- *Standardmäßige Installation*. Bei dieser Variante (das Kontrollkästchen **Installationsparameter ändern** ist deaktiviert) wird das Programm in vollem Umfang mit den von Kaspersky-Lab-Fachleuten empfohlenen Schutzeinstellungen auf Ihrem Computer installiert.

- *Installation mit der Möglichkeit zur Parameteränderung*. In diesem Fall (das Kontrollkästchen **Installationsparameter ändern** ist aktiviert) werden Sie gebeten, einen Installationsordner für das Programm anzugeben und bei Bedarf den Schutz des Installationsprozesses zu aktivieren (s. Abschnitt "Schritt 7. Installationsverzeichnis wählen" auf S. 32) und bei Bedarf den Schutz des Installationsprozesses aktivieren (s. Abschnitt "Schritt 8. Installation vorbereiten" auf S. 32).

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 4. LIZENZVEREINBARUNG ANZEIGEN

In dieser Phase müssen Sie die Lizenzvereinbarung lesen, die zwischen Ihnen und Kaspersky Lab eingegangen wird.

Lesen Sie sich die Vereinbarung sorgfältig durch und wenn Sie mit allen Punkt einverstanden sind, klicken Sie auf die Schaltfläche **Akzeptieren**. Die Installation des Programms auf Ihrem Computer wird fortgesetzt.

Wenn Sie der Lizenzvereinbarung nicht zustimmen, brechen Sie die Programminstallation durch Klick auf **Abbrechen** ab.

SCHRITT 5. ERKLÄRUNG ZUR VERWENDUNG VON KASPERSKY SECURITY NETWORK

Bei diesem Schritt wird Ihnen angeboten, an dem Programm Kaspersky Security Network teilzunehmen. Eine Beteiligung an diesem Programm sieht vor, dass Informationen über auf Ihrem Computer erkannte neue Bedrohungen, über gestartete Programme und über geladene signierte Programme, sowie Systeminformationen an Kaspersky Lab geschickt werden. Es wird dabei garantiert, dass keine persönlichen Daten gesendet werden.

Lesen Sie sich die Erklärung zur Verwendung von Kaspersky Security Network gründlich durch. Um den gesamten Text der Vereinbarung aufzurufen, klicken Sie bitte auf die Schaltfläche **Vollständige KSN-Vereinbarung**. Wenn Sie mit allen Punkten einverstanden sind, setzen Sie im Assistentenfenster das Häkchen im Kontrollkästchen **Ich akzeptiere die Teilnahmebedingungen für Kaspersky Security Network**.

Klicken Sie auf **Weiter**, wenn Sie die Installation mit der Möglichkeit zur Konfigurationsänderung ausführen (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 31). Klicken Sie im Fall einer standardmäßigen Installation auf **Installieren**. Die Installation wird fortgesetzt.

SCHRITT 6. INKOMPATIBLE PROGRAMME SUCHEN

In dieser Phase wird geprüft, ob auf Ihrem Computer Programme installiert sind, die nicht mit Kaspersky Internet Security kompatibel sind.

Wenn keine derartigen Programme gefunden werden, geht der Assistent automatisch zum nächsten Schritt.

Werden inkompatible Programme gefunden, so wird eine entsprechende Liste auf dem Bildschirm angezeigt und Sie werden aufgefordert, die Programme zu entfernen. Programme, die von Kaspersky Internet Security nicht automatisch entfernt werden können, müssen manuell deinstalliert werden. Im Verlauf der Deinstallation inkompatibler Programme wird das System neu gestartet. Anschließend wird die Installation von Kaspersky Internet Security automatisch fortgesetzt.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 7. INSTALLATIONSVERZEICHNIS WÄHLEN

Dieser Schritt des Installationsassistenten ist nur dann verfügbar, wenn die Programminstallation mit der Möglichkeit zur Konfigurationsänderung erfolgt (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 31). Bei der standardmäßigen Installation wird dieser Schritt übersprungen und das Programm wird in dem standardmäßig hierfür vorgesehenen Ordner installiert.

In dieser Phase der Installation wird Ihnen vorgeschlagen, den Ordner zu bestimmen, in den Kaspersky Internet Security installiert wird. Standardmäßig gilt folgender Pfad:

- **<Datenträger>\Program Files\Kaspersky Lab\Kaspersky Internet Security 2011** – für 32-Bit-Systeme.
- **<Datenträger>\Program Files\Kaspersky Lab\Kaspersky Internet Security 2011**– für 64-Bit-Systeme.

Um Kaspersky Internet Security in einem anderen Ordner zu installieren, geben Sie bitte den entsprechenden Pfad im Eingabefeld an oder klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie in dem erscheinenden Fenster den gewünschten Ordner aus.

Bitte beachten Sie die folgenden Einschränkungen:

- Das Programm darf weder auf Netzlaufwerken oder Wechseldatenträgern noch auf virtuelle Laufwerken, die mit dem Befehl `SUBST` erstellt wurden, installiert werden.
- Es wird davor gewarnt, das Programm in einem Ordner zu installieren, der bereits Dateien oder andere Ordner enthält, da der Zugriff auf den Ordner anschließend verboten werden kann.
- Der Pfad des Installationsordners darf höchstens 160 Zeichen lang sein und keines der Sonderzeichen **/**, **?**, **:**, *****, **"**, **>**, **<** und **|** enthalten.

Um festzustellen, ob auf Ihrem Computer ausreichend Speicherplatz für die Installation der Anwendung vorhanden ist, klicken Sie auf die Schaltfläche **Laufwerk**. Das daraufhin erscheinende Fenster enthält Informationen zum verfügbaren Speicherplatz. Um das Fenster zu schließen, klicken Sie auf **OK**.

Zum Fortsetzen der Installation klicken Sie im Fenster des Assistenten auf die Schaltfläche **Weiter**.

SCHRITT 8. INSTALLATION VORBEREITEN

Dieser Schritt des Installationsassistenten ist nur dann verfügbar, wenn die Programminstallation mit der Möglichkeit zur Konfigurationsänderung erfolgt (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 31). Bei der standardmäßigen Installation wird dieser Schritt übersprungen.

Da sich auf Ihrem Computer schädliche Programme befinden können, die fähig sind, die Installation von Kaspersky Internet Security zu stören, muss der Installationsprozess geschützt werden.

Der Schutz des Installationsprozesses ist standardmäßig aktiviert – im Fenster des Assistenten ist das Kontrollkästchen **Installationsprozess schützen** angekreuzt.

Es wird empfohlen, das Kontrollkästchen zu deaktivieren, wenn die Programminstallation andernfalls nicht möglich ist (dies kann beispielsweise bei einer Remote-Installation über Windows Remote Desktop der Fall sein). Der Grund kann im aktivierten Schutz liegen.

Brechen Sie in diesem Fall die Installation ab und starten Sie den Installationsprozess erneut. Aktivieren Sie beim Schritt Installationstyp wählen das Kontrollkästchen **Installationsparameter ändern** (s. Abschnitt "Schritt 3. Installationstyp wählen" auf S. 31) und deaktivieren Sie beim Schritt zur Installationsvorbereitung das Kontrollkästchen **Installationsprozess schützen**.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Installieren**.

Bei der Installation des Programms auf einem Computer mit dem Betriebssystem Microsoft Windows XP werden bestehende Netzwerkverbindungen getrennt. Die Mehrzahl der getrennten Verbindungen wird nach einiger Zeit wiederhergestellt.

SCHRITT 9. INSTALLATION

Die Installation des Programms nimmt einige Zeit in Anspruch. Warten Sie die Fertigstellung ab.

Der Assistent geht nach Abschluss der Installation automatisch zum nächsten Schritt.

Falls bei der Installation ein Fehler auftritt, der möglicherweise durch auf dem Computer vorhandene Schadprogramme verursacht wurde, die eine Installation von Antiviren-Programmen verhindern, schlägt der Installationsassistent vor, die spezielle Uitility *Kaspersky Virus Removal Tool* herunterzuladen, um die Infektion zu beseitigen.

Wenn Sie der Installation des Tools zustimmen, lädt der Installationsassistent es von den Kaspersky-Lab-Servern herunter und startet anschließend automatisch die Installation des Tools. Gelingt dem Assistenten der Download des Tools nicht, so werden Sie aufgefordert, es über einen Link manuell herunterzuladen.

Nachdem das Tool seine Arbeit abgeschlossen hat, muss es entfernt werden. Anschließend wird die Installation von Kaspersky Internet Security erneut gestartet.

SCHRITT 10. PROGRAMM AKTIVIEREN

Durch die *Aktivierung* erlangt die Lizenz für die Nutzung der Vollversion des Programms ihre Gültigkeit für den entsprechenden Zeitraum.

Um das Programm zu aktivieren, ist eine Internetverbindung erforderlich.

Für die Aktivierung von Kaspersky Internet Security bestehen folgende Möglichkeiten:

- **Kommerzielle Version aktivieren**. Wählen Sie diese Option aus und geben Sie den Aktivierungscode (s. Abschnitt "О коде активации" auf S. 43), wenn Sie die kommerzielle Programmversion erworben haben.

  Wenn Sie einen Aktivierungscode für Kaspersky Anti-Virus eingeben, wird nach der Aktivierung eine Umstellung zu Kaspersky Anti-Virus gestartet.

- **Testversion aktivieren**. Wählen Sie diese Aktivierungsvariante, wenn Sie eine Testversion des Programms installieren möchten, bevor Sie über den Kauf einer kommerziellen Version entscheiden. Für die Gültigkeitsdauer der Lizenz für die Testversion können Sie das Programm mit uneingeschränktem Funktionsumfang verwenden. Nach Ablauf der Lizenz ist es nicht möglich, erneut eine Testlizenz zu aktivieren.

- **Später aktivieren**. Bei der Auswahl dieser Variante wird die Aktivierung von Kaspersky Internet Security übersprungen. Das Programm wird auf Ihrem Computer installiert, und Sie haben Zugang zu allen Funktionen außer der Updatefunktion. Ein Update der Antiviren-Datenbanken und der Module von Kaspersky Internet Security können Sie nach der Installation nur ein einziges Mal durchführen. Die Variante **Später aktivieren** steht nur zur Verfügung, wenn der Aktivierungsassistent zum ersten Mal gleich nach der Programminstallation gestartet wird.

SCHRITT 11. ANMELDUNG DES BENUTZERS

Dieser Schritt ist nur bei der Aktivierung einer kommerziellen Programmversion verfügbar. Bei der Aktivierung einer Testversion wird der Schritt übersprungen.

Um auch weiterhin die Möglichkeit zu haben, den Technischen Support von Kaspersky Lab zu kontaktieren, müssen Sie sich registrieren.

Wenn Sie mit der Anmeldung einverstanden sind, füllen Sie die entsprechenden Felder aus und klicken Sie dann auf **Weiter**, um Ihre Anmeldung abzuschicken.

SCHRITT 12. AKTIVIERUNG ABSCHLIEßEN

Der Assistent informiert Sie über den erfolgreichen Abschluss der Aktivierung von Kaspersky Internet Security. Außerdem werden Informationen über die Lizenz angezeigt: Typ (kommerziell oder Test), Gültigkeitsdauer der Lizenz, sowie Anzahl der Computer, für die die Lizenz gültig ist.

Bei der Aktivierung eines Abonnements werden anstelle des Ablaufdatums für die Lizenz Informationen zum Abo-Status (s. Abschnitt "Varianten für den Abo-Status" auf S. 211) angezeigt.

Klicken Sie auf den Link **Weiter**, um den Assistenten fortzusetzen.

SCHRITT 13. SYSTEMANALYSE

Auf dieser Etappe werden Informationen über Programme, die zu Microsoft Windows gehören, gesammelt. Diese Programme werden in die Liste der vertrauenswürdigen Anwendungen aufgenommen, deren Aktionen im System nicht beschränkt werden.

Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

SCHRITT 14. ASSISTENT ABSCHLIEßEN

Das letzte Fenster des Assistenten informiert über den Abschluss der Programminstallation. Um mit der Arbeit von Kaspersky Internet Security zu beginnen, vergewissern Sie sich, dass das Kontrollkästchen **Kaspersky Internet Security starten** aktiviert ist und klicken Sie auf **Beenden**.

In einigen Fällen kann ein Neustart des Betriebssystems erforderlich sein. Wenn das Kontrollkästchen **Kaspersky Internet Security starten** aktiviert ist, wird das Programm nach einem Reboot automatisch gestartet.

Wenn Sie das Kontrollkästchen vor dem Abschluss des Assistenten deaktiviert haben, muss das Programm manuell gestartet werden (s. Abschnitt "Programm manuell starten und beenden" auf S. 54).

AKTUALISIERUNG EINER VORGÄNGERVERSION VON KASPERSKY INTERNET SECURITY

Wenn Kaspersky Internet Security 2010 bereits auf Ihrem Computer installiert ist, müssen Sie das Programm auf die Version Kaspersky Internet Security 2011 updaten. Bei Vorhandensein einer gültigen Lizenz für Kaspersky Internet Security 2010 müssen Sie das Programm nicht aktivieren: Der Installationsassistent erhält automatisch die Informationen über die Lizenz für Kaspersky Internet Security 2010 und verwendet diese beim Installationsvorgang.

Kaspersky Internet Security wird auf dem Computer interaktiv mit einem Installationsassistenten installiert.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Wird das Programm für den Schutz von mehr als einem Computer verwendet, so geht die Installation auf allen Computern identisch vor sich. Hierbei ist zu beachten, dass die Gültigkeitsdauer der Lizenz gemäß Lizenzvereinbarung mit der ersten Aktivierung des Programms beginnt.

- *Zur Installation von Kaspersky Internet Security auf Ihrem Computer,*

  starten Sie auf der Produkt-CD die Installationsdatei (Datei mit der Erweiterung .exe).

  Der Installationsvorgang für das Programm Kaspersky Internet Security, das aus dem Internet bezogen wurde, ist identisch mit dem Installationsvorgang von der CD-ROM.

IN DIESEM ABSCHNITT

Schritt 1. Nach neuer Programmversion suchen 35

Schritt 2. Systemkompatibilität für Installation prüfen 36

Schritt 3. Installationstyp wählen 36

Schritt 4. Lizenzvereinbarung anzeigen 36

Schritt 5. Erklärung zur Verwendung von Kaspersky Security Network 36

Schritt 6. Inkompatible Programme suchen 37

Schritt 7. Installationsverzeichnis wählen 37

Schritt 8. Installation vorbereiten 38

Schritt 9. Installation 38

Schritt 10. Aktivierung abschließen 38

Schritt 11. Systemanalyse 39

Schritt 12. Assistent abschließen 39

SCHRITT 1. NACH NEUER PROGRAMMVERSION SUCHEN

Vor der Installation wird geprüft, ob neuere Versionen von Kaspersky Internet Security auf den Updateservern von Kaspersky Lab vorhanden sind.

Wenn keine neuere Version des Programms auf den Updateservern von Kaspersky Lab gefunden wurde, wird der Installationsassistent für diese Version gestartet.

Wenn auf den Updateservern eine neuere Version von Kaspersky Internet Security vorgefunden wurde, werden Ihnen Download und Installation vorgeschlagen. Es wird empfohlen, die neue Programmversion zu installieren, da neue Versionen den Schutz Ihres Computers optimieren. Sollten Sie die neuere Version ablehnen, wird der Installationsassistent der laufenden Version gestartet. Sollten Sie die Installation der neueren Version annehmen, werden die Programmdateien auf Ihren Computer kopiert und der Installationsassistent wird automatisch gestartet. Eine weitere Beschreibung zur Installation einer neueren Version finden Sie in der Dokumentation zur entsprechenden Programmversion.

SCHRITT 2. SYSTEMKOMPATIBILITÄT FÜR INSTALLATION PRÜFEN

Vor der Installation von Kaspersky Internet Security auf Ihrem Computer wird die Kompatibilität des Betriebssystems und der Service Packs mit den Softwarevoraussetzungen für die Installation abgeglichen Softwarevoraussetzungen für die Installation (s. Abschnitt "Hard- und Softwarevoraussetzungen" auf S. 28). Außerdem werden die Hardwarevoraussetzungen geprüft sowie die Rechte für die Installation des Programms. Wenn eine der aufgezählten Bedingung nicht erfüllt wird, erscheint eine entsprechende Meldung auf dem Bildschirm.

Wenn der Computer die Voraussetzungen erfüllt, sucht der Assistent nach Kaspersky-Lab-Programmen, deren gleichzeitige Verwendung mit Kaspersky Internet Security zu Konflikten führen kann. Wenn solche Programme gefunden werden, werden Sie aufgefordert, die Programme manuell zu entfernen.

Wenn sich unter den gefundenen Programmen eine Vorgängerversion von Kaspersky Anti-Virus oder Kaspersky Internet Security befindet, werden alle Daten, die von Kaspersky Internet Security 2011 verwendet werden können (Aktivierungsdaten, Programmeinstellungen usw.), gespeichert und das bereits installierte Programm wird automatisch gelöscht.

SCHRITT 3. INSTALLATIONSTYP WÄHLEN

In dieser Phase der Installation können Sie einen passenden Typ für die Installation von Kaspersky Internet Security auswählen:

- *Standardmäßige Installation*. Bei dieser Variante (das Kontrollkästchen **Installationsparameter ändern** ist deaktiviert) wird das Programm in vollem Umfang mit den von Kaspersky-Lab-Fachleuten empfohlenen Schutzeinstellungen auf Ihrem Computer installiert.

- *Installation mit der Möglichkeit zur Parameteränderung*. In diesem Fall (das Kontrollkästchen **Installationsparameter ändern** ist aktiviert) werden Sie gebeten, einen Installationsordner für das Programm anzugeben und bei Bedarf den Schutz des Installationsprozesses zu aktivieren (s. Abschnitt "Schritt 7. Installationsverzeichnis wählen" auf S. 32) und bei Bedarf den Schutz des Installationsprozesses aktivieren (s. Abschnitt "Schritt 8. Installation vorbereiten" auf S. 32).

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 4. LIZENZVEREINBARUNG ANZEIGEN

In dieser Phase müssen Sie die Lizenzvereinbarung lesen, die zwischen Ihnen und Kaspersky Lab eingegangen wird.

Lesen Sie sich die Vereinbarung sorgfältig durch und wenn Sie mit allen Punkt einverstanden sind, klicken Sie auf die Schaltfläche **Akzeptieren**. Die Installation des Programms auf Ihrem Computer wird fortgesetzt.

Wenn Sie der Lizenzvereinbarung nicht zustimmen, brechen Sie die Programminstallation durch Klick auf **Abbrechen** ab.

SCHRITT 5. ERKLÄRUNG ZUR VERWENDUNG VON KASPERSKY SECURITY NETWORK

Bei diesem Schritt wird Ihnen angeboten, an dem Programm Kaspersky Security Network teilzunehmen. Eine Beteiligung an diesem Programm sieht vor, dass Informationen über auf Ihrem Computer erkannte neue Bedrohungen, über gestartete Programme und über geladene signierte Programme, sowie Systeminformationen an Kaspersky Lab geschickt werden. Es wird dabei garantiert, dass keine persönlichen Daten gesendet werden.

Lesen Sie sich die Erklärung zur Verwendung von Kaspersky Security Network gründlich durch. Um den gesamten Text der Vereinbarung aufzurufen, klicken Sie bitte auf die Schaltfläche **Vollständige KSN-Vereinbarung**. Wenn Sie mit allen Punkten einverstanden sind, setzen Sie im Assistentenfenster das Häkchen im Kontrollkästchen **Ich akzeptiere die Teilnahmebedingungen für Kaspersky Security Network**.

Klicken Sie auf **Weiter**, wenn Sie die Installation mit der Möglichkeit zur Konfigurationsänderung ausführen (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 31). Klicken Sie im Fall einer standardmäßigen Installation auf **Installieren**. Die Installation wird fortgesetzt.

SCHRITT 6. INKOMPATIBLE PROGRAMME SUCHEN

In dieser Phase wird geprüft, ob auf Ihrem Computer Programme installiert sind, die nicht mit Kaspersky Internet Security kompatibel sind.

Wenn keine derartigen Programme gefunden werden, geht der Assistent automatisch zum nächsten Schritt.

Werden inkompatible Programme gefunden, so wird eine entsprechende Liste auf dem Bildschirm angezeigt und Sie werden aufgefordert, die Programme zu entfernen. Programme, die von Kaspersky Internet Security nicht automatisch entfernt werden können, müssen manuell deinstalliert werden. Im Verlauf der Deinstallation inkompatibler Programme wird das System neu gestartet. Anschließend wird die Installation von Kaspersky Internet Security automatisch fortgesetzt.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 7. INSTALLATIONSVERZEICHNIS WÄHLEN

Dieser Schritt des Installationsassistenten ist nur dann verfügbar, wenn die Programminstallation mit der Möglichkeit zur Konfigurationsänderung erfolgt (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 31). Bei der standardmäßigen Installation wird dieser Schritt übersprungen und das Programm wird in dem standardmäßig hierfür vorgesehenen Ordner installiert.

In dieser Phase der Installation wird Ihnen vorgeschlagen, den Ordner zu bestimmen, in den Kaspersky Internet Security installiert wird. Standardmäßig gilt folgender Pfad:

- **<Datenträger>\Program Files\Kaspersky Lab\Kaspersky Internet Security 2011** – für 32-Bit-Systeme.
- **<Datenträger>\Program Files\Kaspersky Lab\Kaspersky Internet Security 2011**– für 64-Bit-Systeme.

Um Kaspersky Internet Security in einem anderen Ordner zu installieren, geben Sie bitte den entsprechenden Pfad im Eingabefeld an oder klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie in dem erscheinenden Fenster den gewünschten Ordner aus.

Bitte beachten Sie die folgenden Einschränkungen:

- Das Programm darf weder auf Netzlaufwerken oder Wechseldatenträgern noch auf virtuelle Laufwerken, die mit dem Befehl `SUBST` erstellt wurden, installiert werden.
- Es wird davor gewarnt, das Programm in einem Ordner zu installieren, der bereits Dateien oder andere Ordner enthält, da der Zugriff auf den Ordner anschließend verboten werden kann.
- Der Pfad des Installationsordners darf höchstens 160 Zeichen lang sein und keines der Sonderzeichen **/**, **?**, **:**, *****, **"**, **>**, **<** und **|** enthalten.

Um festzustellen, ob auf Ihrem Computer ausreichend Speicherplatz für die Installation der Anwendung vorhanden ist, klicken Sie auf die Schaltfläche **Laufwerk**. Das daraufhin erscheinende Fenster enthält Informationen zum verfügbaren Speicherplatz. Um das Fenster zu schließen, klicken Sie auf **OK**.

Zum Fortsetzen der Installation klicken Sie im Fenster des Assistenten auf die Schaltfläche **Weiter**.

SCHRITT 8. INSTALLATION VORBEREITEN

Dieser Schritt des Installationsassistenten ist nur dann verfügbar, wenn die Programminstallation mit der Möglichkeit zur Konfigurationsänderung erfolgt (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 31). Bei der standardmäßigen Installation wird dieser Schritt übersprungen.

Da sich auf Ihrem Computer schädliche Programme befinden können, die fähig sind, die Installation von Kaspersky Internet Security zu stören, muss der Installationsprozess geschützt werden.

Der Schutz des Installationsprozesses ist standardmäßig aktiviert – im Fenster des Assistenten ist das Kontrollkästchen **Installationsprozess schützen** angekreuzt.

Es wird empfohlen, das Kontrollkästchen zu deaktivieren, wenn die Programminstallation andernfalls nicht möglich ist (dies kann beispielsweise bei einer Remote-Installation über Windows Remote Desktop der Fall sein). Der Grund kann im aktivierten Schutz liegen.

Brechen Sie in diesem Fall die Installation ab und starten Sie den Installationsprozess erneut. Aktivieren Sie beim Schritt Installationstyp wählen das Kontrollkästchen **Installationsparameter ändern** (s. Abschnitt "Schritt 3. Installationstyp wählen" auf S. 31) und deaktivieren Sie beim Schritt zur Installationsvorbereitung das Kontrollkästchen **Installationsprozess schützen**.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Installieren**.

Bei der Installation des Programms auf einem Computer mit dem Betriebssystem Microsoft Windows XP werden bestehende Netzwerkverbindungen getrennt. Die Mehrzahl der getrennten Verbindungen wird nach einiger Zeit wiederhergestellt.

SCHRITT 9. INSTALLATION

Die Installation des Programms nimmt einige Zeit in Anspruch. Warten Sie die Fertigstellung ab.

Der Assistent geht nach Abschluss der Installation automatisch zum nächsten Schritt.

Falls bei der Installation ein Fehler auftritt, der möglicherweise durch auf dem Computer vorhandene Schadprogramme verursacht wurde, die eine Installation von Antiviren-Programmen verhindern, schlägt der Installationsassistent vor, die spezielle Uitility *Kaspersky Virus Removal Tool* herunterzuladen, um die Infektion zu beseitigen.

Wenn Sie der Installation des Tools zustimmen, lädt der Installationsassistent es von den Kaspersky-Lab-Servern herunter und startet anschließend automatisch die Installation des Tools. Gelingt dem Assistenten der Download des Tools nicht, so werden Sie aufgefordert, es über einen Link manuell herunterzuladen.

Nachdem das Tool seine Arbeit abgeschlossen hat, muss es entfernt werden. Anschließend wird die Installation von Kaspersky Internet Security erneut gestartet.

SCHRITT 10. AKTIVIERUNG ABSCHLIEßEN

Der Assistent informiert Sie über den erfolgreichen Abschluss der Aktivierung von Kaspersky Internet Security. Außerdem werden Informationen über die Lizenz angezeigt: Typ (kommerziell oder Test), Gültigkeitsdauer der Lizenz, sowie Anzahl der Computer, für die die Lizenz gültig ist.

Bei der Aktivierung eines Abonnements werden anstelle des Ablaufdatums für die Lizenz Informationen zum Abo-Status (s. Abschnitt "Varianten für den Abo-Status" auf S. 211) angezeigt.

Klicken Sie auf den Link **Weiter**, um den Assistenten fortzusetzen.

SCHRITT 11. SYSTEMANALYSE

Auf dieser Etappe werden Informationen über Programme, die zu Microsoft Windows gehören, gesammelt. Diese Programme werden in die Liste der vertrauenswürdigen Anwendungen aufgenommen, deren Aktionen im System nicht beschränkt werden.

Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

SCHRITT 12. ASSISTENT ABSCHLIEßEN

Das letzte Fenster des Assistenten informiert über den Abschluss der Programminstallation. Um mit der Arbeit von Kaspersky Internet Security zu beginnen, vergewissern Sie sich, dass das Kontrollkästchen **Kaspersky Internet Security starten** aktiviert ist und klicken Sie auf **Beenden**.

In einigen Fällen kann ein Neustart des Betriebssystems erforderlich sein. Wenn das Kontrollkästchen **Kaspersky Internet Security starten** aktiviert ist, wird das Programm nach einem Reboot automatisch gestartet.

Wenn Sie das Kontrollkästchen vor dem Abschluss des Assistenten deaktiviert haben, muss das Programm manuell gestartet werden (s. Abschnitt "Programm manuell starten und beenden" auf S. 54).

UNTYPISCHE INSTALLATIONSSZENARIEN

In diesem Abschnitt sind Szenarien für die Programminstallation beschrieben, die von der Standard-Installation oder vom Update auf Basis der Vorgängerversion abweichen.

Installation von Kaspersky Internet Security mit anschließender Aktivierung mittels Aktivierungscode von Kaspersky Anti-Virus

Wenn Sie während der Installation von Kaspersky Internet Security bei der Programmaktivierung einen Aktivierungscode für Kaspersky Anti-Virus eingeben, startet ein Vorgang, bei dem Kaspersky Anti-Virus auf Ihrem Computer installiert wird.

Wenn Sie während der Installation von Kaspersky Internet Security bei der Programmaktivierung die Option **Später aktivieren** wählen, und das installierte Programm dann mit einem Aktivierungscode für Kaspersky Anti-Virus aktivieren, startet ebenfalls eine Vorgang, bei dem Kaspersky Anti-Virus auf Ihrem Computer installiert wird.

Installation von Kaspersky Internet Security 2011 über Kaspersky Anti-Virus 2010

Wenn Sie die Installation von Kaspersky Internet Security 2011 auf einem Computer starten, auf dem bereits Kaspersky Anti-Virus 2010 mit einer gültigen Lizenz aktiviert ist, schlägt Ihnen der Installationsassistent nach Erkennung der Lizenz folgende Optionen für das weitere Vorgehen vor:

- Verwendung der gültigen Lizenz von Kaspersky Anti-Virus 2010. In diesem Fall wird ein Vorgang gestartet, bei dem Kaspersky Anti-Virus 2011 auf Ihrem Computer installiert wird. Sie können Kaspersky Anti-Virus 2011 für die gesamte Lizenzlaufzeit von Kaspersky Anti-Virus 2010 verwenden.

- Fortsetzen der Installation von Kaspersky Internet Security 2011. In diesem Fall wird der Installationsvorgang nach dem Standard-Szenario fortgesetzt und beginnt mit der Programmaktivierung.

ERSTE SCHRITTE

Nach abgeschlossener Installation und Konfiguration ist das Programm einsatzbereit. Um einen effektiven Schutz Ihres Computers zu gewährleisten, empfehlen wir direkt im Anschluss an die Installation und Konfiguration die Durchführung folgender Aktionen:

- Programm-Datenbanken aktualisieren (s. Abschnitt "Aktualisierung von Programmdatenbanken und -modulen" auf S. 62).
- Computer auf Viren untersuchen (s. Abschnitt "Wie eine vollständige Virenuntersuchung des Computers ausgeführt wird" auf S. 65) und auf Schwachstellen untersuchen (s. Abschnitt "Wie der Computer auf Schwachstellen untersucht wird" auf S. 66).
- Schutzstatus des Computers prüfen (auf S. 55) und bei Bedarf Probleme im Schutz beheben (s. Abschnitt "Probleme im Computerschutz diagnostizieren und beheben" auf S. 55).

PROGRAMM DEINSTALLIEREN.

Wenn Kaspersky Internet Security deinstalliert wird, sind der Computer und Ihre persönlichen Daten ungeschützt!

Kaspersky Internet Security wird mit dem Installationsassistenten entfernt.

Gehen Sie folgendermaßen vor, den Assistenten zu starten:

1. Wählen Sie im **Startmenü** auf **Programme** → **Kaspersky Internet Security 2011** → **Reparieren oder Löschen**.
2. Klicken Sie im folgenden Fenster auf **Löschen**.

IN DIESEM ABSCHNITT

Schritt 1. Daten zur erneuten Verwendung speichern 40

Schritt 2. Programmdeinstallation bestätigen 41

Schritt 3. Programm deinstallieren. Deinstallation abschließen 41

SCHRITT 1. DATEN ZUR ERNEUTEN VERWENDUNG SPEICHERN

Bei diesem Schritt können Sie festlegen, welche vom Programm verwendeten Daten Sie speichern möchten, um sie später bei einer Neuinstallation des Programms (z.B. Installation einer neueren Version) wiederzuverwenden.

In der Grundeinstellung wird das Programm vollständig vom Computer entfernt.

Gehen Sie folgendermaßen vor, um bestimmte Daten zur erneuten Verwendung zu speichern:

1. Wählen Sie die Variante **Objekte der Anwendung speichern**.
2. Aktivieren Sie die Kontrollkästchen der Daten, die gespeichert werden sollen.
   - **Aktivierungsdaten** – Daten, die es erlauben, das zu installierende Programm später nicht zu aktivieren, sondern automatisch die aktive Lizenz zu verwenden, vorausgesetzt, sie zum Zeitpunkt der Installation noch gültig ist.

- **Anti-Spam-Datenbanken** – Datenbanken, die Muster von Spam-Mails enthalten, die das Program bei seiner Arbeit erhalten und gespeichert hat.
- **Backup- und Quarantäneobjekte** – Dateien, die vom Programm untersucht und im Backup und in der Quarantäne gespeichert wurden.
- **Funktionsparameter des Programms** – Parameterwerte für die Programmfunktion, die im Verlauf der Programmkonfiguration eingestellt wurden.
- **iSwift und iChecker-Daten** – Dateien mit Informationen zu den Objekten, die bereits auf Viren untersucht wurden.
- **Daten des gemeinsamen Ordners der Sicheren Umgebung** – Dateien, die bei der Arbeit in der Sicheren Umgebung in einem speziellen Ordner gespeichert wurden, der auch in der normalen Umgebung verfügbar ist.

SCHRITT 2. PROGRAMMDEINSTALLATION BESTÄTIGEN

Da durch eine Programmdeinstallation der Schutz Ihres Computers und Ihrer persönlichen Daten gefährdet werden kann, muss das Löschen des Programms bestätigt werden. Klicken Sie dazu auf die Schaltfläche **OK**.

Bevor die Deinstallation abgeschlossen wird, können Sie diese Aktion jederzeit durch Klick auf **Abbrechen** verwerfen.

SCHRITT 3. PROGRAMM DEINSTALLIEREN. DEINSTALLATION ABSCHLIEßEN

Bei diesem Schritt löscht der Assistent das Programm von Ihrem Computer. Warten Sie, bis der Deinstallationsvorgang abgeschlossen wird.

Im Verlauf der Deinstallation kann ein Neustart des Systems erforderlich sein. Wenn Sie einen sofortigen Neustart ablehnen, wird der Abschluss der Deinstallation aufgeschoben, bis das Betriebssystem neu gestartet oder der Computer herunter- und hochgefahren wird.

LIZENZVERWALTUNG

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmlizenzierung zusammenhängen. In diesem Abschnitt erfahren Sie außerdem, wie die Gültigkeitsdauer für eine Lizenz automatisch verlängert werden kann und wo sich Informationen zur aktiven Lizenz befinden.

IN DIESEM ABSCHNITT

Über den Lizenzvertrag 42

Über die Lizenz 42

Über den Aktivierungscode 43

Lizenz-Info anzeigen 44

ÜBER DEN LIZENZVERTRAG

Der *Lizenzvertrag* ist ein Vertrag zwischen einer natürlichen oder juristischen Person, die rechtmäßiger Besitzer eines Exemplars von Kaspersky Internet Security ist, und der Kaspersky Lab ZAO. Der Lizenzvertrag gehört zum Lieferumfang jedes Kaspersky-Lab-Programms. Er legt die Rechte und Einschränkungen für die Nutzung von Kaspersky Internet Security genau fest.

In Übereinstimmung mit dem Lizenzvertrag erhalten Sie durch den Erwerb und die Installation eines Kaspersky-Lab-Programms das unbefristete Besitzrecht an einer Kopie.

ÜBER DIE LIZENZ

Die *Lizenz* verleiht das Recht zur Nutzung von Kaspersky Internet Security und der zum Programm gehörenden Zusatzleistungen, die von Kaspersky Lab und seinen Partnern angeboten werden.

Jede Lizenz wird durch Gültigkeitsdauer und Typ charakterisiert.

Die *Gültigkeitsdauer einer Lizenz* ist die Zeitspanne, für die Ihnen die Zusatzleistungen zur Verfügung stehen.

- Technischer Support.
- Update der Datenbanken und Module des Programms.

Der Umfang der angebotenen Leistungen ist vom Lizenztyp abhängig.

Es sind folgende Lizenztypen vorgesehen

- *Test* – Kostenlose Lizenz mit begrenzter Gültigkeitsdauer (z.B. 30 Tage) zum Kennenlernen von Kaspersky Internet Security.

  Eine Testlizenz kann nur einmal verwendet werden und ihr Einsatz ist nach der Verwendung einer kommerziellen Lizenz nicht mehr möglich!

  Eine Testlizenz wird zusammen mit einer Testversion des Programms geliefert. Wenn Sie eine Testlizenz verwenden, ist der Technische Support auf Fragen über die Programmaktivierung und den Kauf einer kommerziellen Lizenz beschränkt. Nach Ablauf der Gültigkeitsdauer einer Testlizenz stellt Kaspersky Internet

Security alle Funktionen ein. Um mit dem Programm weiterzuarbeiten, ist eine Aktivierung notwendig (s. Abschnitt "Wie das Programm aktiviert wird" auf S. 60).

- *Kommerziell* – Gekaufte Lizenz, die eine begrenzte Gültigkeitsdauer (z.B. 1 Jahr) besitzt und beim Kauf von Kaspersky Internet Security zur Verfügung gestellt wird. Für jede Lizenz ist eine bestimmte Anzahl von Computern festgelegt, auf der Kaspersky Internet Security mit dieser Lizenz installiert werden darf.

  Während der Laufzeit einer kommerziellen Lizenz sind alle Programmfunktionen und zusätzliche Services verfügbar.

  Nach Ablauf der Gültigkeitsdauer einer kommerziellen Lizenz führt Kaspersky Internet Security seine Funktionen weiterhin aus, allerdings werden die Antiviren-Datenbanken nicht mehr aktualisiert. Sie können Ihren Computer weiterhin auf Viren untersuchen und die Schutzkomponenten verwenden, jedoch nur mit den Antiviren-Datenbanken , die bei Ablauf der Lizenz aktuell waren. Sie werden zwei Wochen vor Ablauf der Lizenz vom Programm benachrichtigt und können rechtzeitig die Gültgkeitsdauer der Lizenz verlängern (s. Abschnitt "Lizenzerwerb oder -verlängerung" auf S. 61).

- *Kommerzielle Lizenz mit Update-Abonnement* und *kommerzielle Update- und Schutz-Lizenz* – Gekaufte Lizenz mit flexiblen Einsatzmöglichkeiten: Sie können das Abonnement anhalten und fortsetzen, die Gültigkeitsdauer des Abos im automatischen Modus verlängern oder das Abo kündigen. Eine Lizenz mit Abonnement wird von Dienstleistern angeboten. Das Abonnement wird über den persönlichen Bereich des Benutzers auf der Webseite des Dienstleisters verwaltet.

  Ein Abonnement kann eine begrenzte Laufzeit besitzen (z.B. für 1 Jahr) oder unbegrenzt sein. Ein Abonnement mit begrenzter Laufzeit muss bei Ablauf der Gültigkeitsdauer vom Benutzer verlängert werden. Ein Abonnement mit unbegrenzter Laufzeit wird automatisch verlängert, falls der erforderliche Betrag rechtzeitig an den Dienstleister überwiesen wird.

  Wenn die Abonnementlaufzeit begrenzt ist, wird Ihnen eine Ermässigungsfrist zur Verlängerung des Abos eingeräumt, während der die Funktionsfähigkeit des Programms erhalten bleibt.

  Wenn ein Abonnement nicht verlängert wird, lädt Kaspersky Internet Security nach Ablauf der Ermäßigungsfrist keine Updates für die Programm-Datenbanken mehr herunter (für eine Lizenz mit Update-Abonnement), stellt den Computerschutz ein und startet keine Untersuchungsaufgaben (für eine Lizenz mit Update- und Schutz-Abonnement).

  Bei Verwendung eines Abonnements können Sie keinen anderen Aktivierungscode verwenden, um die Gültigkeit einer Lizenz zu verlängern. Das ist erst nach Ablauf des Abonnements möglich.

  Wenn im Augenblick der Abonnementsaktivierung eine Lizenz mit beschränkter Gültigkeitsdauer aktiviert wurde, wird diese durch eine neue Lizenz mit Abonnement ersetzt. Um ein Abonnement zu kündigen, wenden Sie sich an den Dienstleister, bei dem Sie Kaspersky Internet Security erworben haben.

  Abhängig vom Händler können die Aktionen mit dem Abonnement (s. Abschnitt "Varianten für den Abo-Status" auf S. 211) unterschiedlich sein. Außerdem kann es sein, dass Ihnen keine Ermässigungsfrist gewährt wird, während der das Abo verlängert werden kann.

ÜBER DEN AKTIVIERUNGSCODE

Ein *Aktivierungscode* ist ein Code, den Sie beim Kauf einer kommerziellen Lizenz für Kaspersky Internet Security erhalten. Dieser Code ist für die Programmaktivierung erforderlich.

Der Aktivierungscode besteht aus einer durch Bindestriche getrennten Folge von lateinischen Buchstaben und Ziffern, die in vier Blöcken zu je fünf Zeichen angeordnet sind (Beispiel: AA111-AA111-AA111-AA111).

LIZENZ-INFO ANZEIGEN

Gehen Sie folgendermaßen vor, um Informationen zur aktiven Lizenz anzuzeigen:

1. Öffnen Sie das Programmhauptfenster.

2. Öffnen Sie mit dem Link **Lizenz** im unteren Fensterbereich das Fenster **Lizenzverwaltung**.

   In diesem Fenster können Sie den Vorgang zur Programmaktivierung starten (s. Abschnitt "Wie wird das Programm aktiviert?" auf S. 60), eine neue Lizenz erwerben oder die Gültigkeitsdauer für die aktive Lizenz verlängern (s. Abschnitt "Lizenzerwerb oder -verlängerung" auf S. 61).

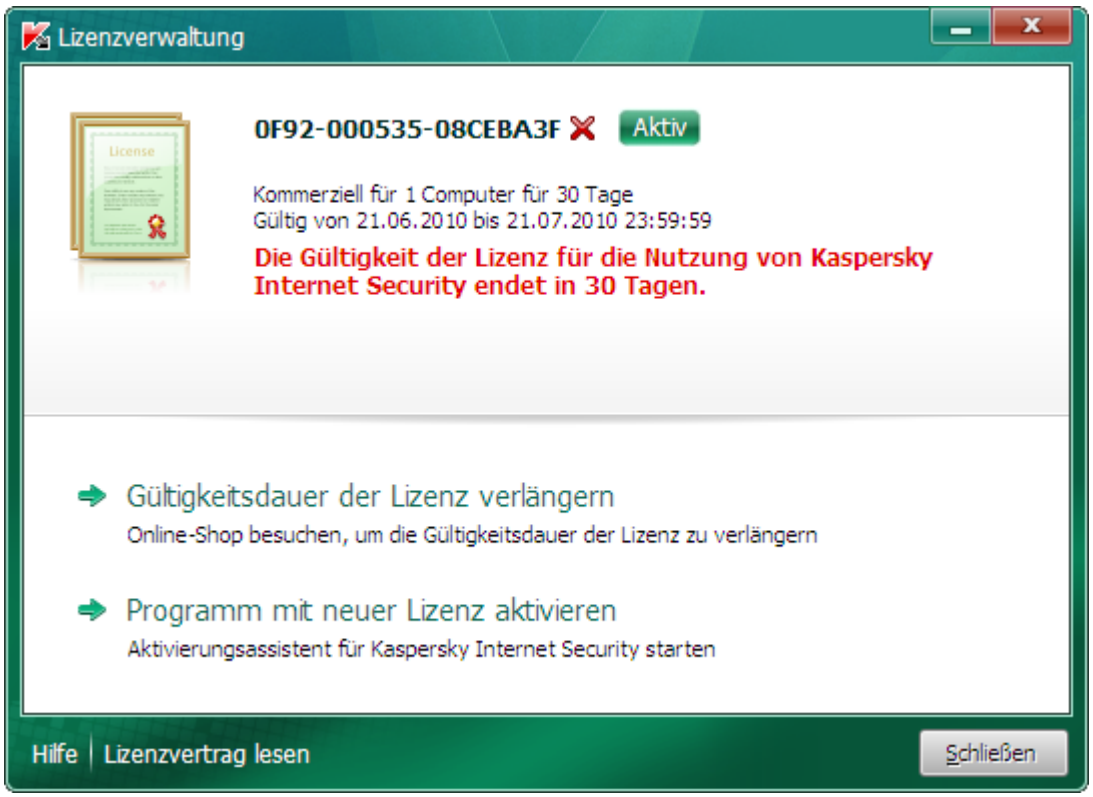
Lizenzverwaltung
0F92-000535-08CEBA3F
Aktiv
Kommerziell für 1 Computer für 30 Tage
Gültig von 21.06.2010 bis 21.07.2010 23:59:59
Die Gültigkeit der Lizenz für die Nutzung von Kaspersky Internet Security endet in 30 Tagen.
Gültigkeitsdauer der Lizenz verlängern
Online-Shop besuchen, um die Gültigkeitsdauer der Lizenz zu verlängern
Programm mit neuer Lizenz aktivieren
Aktivierungsassistent für Kaspersky Internet Security starten
Hilfe
Lizenzvertrag lesen
Schließen

Abbildung 1. Fenster Lizenzen verwalten

PROGRAMMOBERFLÄCHE

Kaspersky Internet Security bietet eine intuitive bedienbare und komfortable Oberfläche. In diesem Abschnitt werden ihre wichtigsten Elemente ausführlich beschrieben.

Kaspersky Internet Security verfügt über Erweiterungskomponenten (Plug-ins), die in folgende Programme integriert werden können: Microsoft Office Outlook, Microsoft Outlook Express, The Bat!, Thunderbird, Mozilla Firefox, Microsoft Internet Explorer und Microsoft Windows Explorer. Die Plug-ins erweitern die Möglichkeiten der genannten Programme, weil die Steuerung und Konfiguration der Programmkomponenten direkt aus ihrem Interface möglich ist.

IN DIESEM ABSCHNITT

Symbol im Infobereich der Taskleiste 45

Kontextmenü 46

Hauptfenster von Kaspersky Internet Security 47

Meldungsfenster und Popupmeldungen 50

Programmkonfigurationsfenster 52

Kaspersky Gadget 53

SYMBOL IM INFOBEREICH DER TASKLEISTE

Sofort nach der Installation von Kaspersky Internet Security erscheint sein Symbol im Infobereich der Taskleiste von Microsoft Windows.

Unter dem Betriebssystem Microsoft Windows 7 ist das Programmsymbol standardmäßig ausgeblendet, wobei es für die Arbeit mit dem Programm jedoch eingeblendet werden kann (s. Dokumentation des Betriebssystems).

Das Symbol besitzt folgende Funktionen:

- Es dient als Indikator für die Arbeit des Programms.
- Es bietet Zugriff auf das Kontextmenü, das Programmhauptfenster und das Nachrichtenfenster.

Indikator für die Programmarbeit

Das Symbol dient als Indikator für die Arbeit des Programms. Es informiert über den Schutzstatus und zeigt eine Reihe wichtiger Aktionen, die vom Programm ausgeführt werden.

– Es wird eine E-Mail-Nachricht untersucht.

– Der Web-Datenverkehr wird untersucht.

– Die Datenbanken und Programm-Module werden aktualisiert.

– Ein Neustart des Computers ist erforderlich, um die Updates zu übernehmen.

– Bei der Arbeit einer Programmkomponente ist eine Störung aufgetreten.

Die Animation des Symbols ist standardmäßig aktiviert: Beispielsweise erscheint bei der Untersuchung einer E-Mail im Hintergrund des Programmsymbols das Piktogramm eines Briefs, beim Update der Programm-Datenbanken erscheint ein rotierender Globus. Sie können die Animation ausschalten (s. Abschnitt "Aktive Elemente der Benutzeroberfläche" auf S. 198).

Wenn die Animation aktiviert ist, kann das Symbol folgendes Aussehen annehmen:

(farbiges Symbol) – Alle oder einige Schutzkomponenten sind aktiv.

(schwarzweißes Symbol) – Alle Schutzkomponenten wurden deaktiviert.

Zugriff auf das Kontextmenü und auf die Programmfenster

Mit Hilfe des Symbols können Sie das Kontextmenü (auf S. 46) und das Programmhauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47) öffnen.

- *Um das Kontextmenü zu öffnen,*

  zeigen Sie mit der Maus auf das Symbol und führen Sie einen Rechtsklick aus.

- *Um das Programmhauptfenster zu öffnen:*

  zeigen Sie mit der Maus auf das Symbol und führen Sie einen Linksklick aus.

Wenn Nachrichten von Kaspersky Lab erschienen sind, wird im Infobereich der Taskleiste von Microsoft Windows das Symbol eingeblendet. Das Fenster für den News Agent (s. Abschnitt "News Agent" auf S. 198) kann durch Doppelklick auf dieses Symbol geöffnet werden.

KONTEXTMENÜ

Das Kontextmenü bietet Zugriff auf die wichtigsten Schutzaufgaben.

Das Menü von Kaspersky Internet Security enthält folgende Punkte:

- **Update** – startet die Aktualisierung der Programmdatenbanken und -module.
- **Tools** – Öffnet ein Kontextmenü, das folgende Punkte enthält:
  - **Programmkontrolle** – öffnet das Fenster **Programmaktivität**;
  - **Netzwerkmonitor** – öffnet das Fenster **Netzwerkmonitor**;
  - **Virtuelle Tastatur** – zeigt die virtuelle Tastatur auf dem Bildschirm an.
- **Sicherer Programmstart** – startet einen sicheren Desktop für die Arbeit mit Programmen, die Ihrer Einschätzung nach unsicher sein können. Ist der sichere Desktop bereits gestartet, wird zu diesem gewechselt.

  Bei der Arbeit auf dem sicheren Desktop heißt dieser Menüpunkt **Zum normalen Desktop** und dient dazu, zum Standard-Desktop zu wechseln.
- **Kaspersky Internet Security** – Programmhauptfenster öffnen.
- **Schutz anhalten / Schutz fortsetzen** – Arbeit der Echtzeitschutz-Komponenten vorübergehend deaktivieren / wieder aktivieren. Dieser Menüpunkt bezieht sich nicht auf das Programm-Update und die Ausführung von Aufgaben zur Virensuche.
- **Kindersicherung aktivieren / Kindersicherung deaktivieren** – aktiviert / deaktiviert die Kindersicherung für das aktuelle Benutzerkonto.

- **Einstellungen** – öffnet das Fenster zur Konfiguration der Funktionsparameter des Programms.
- **Über das Programm** – Infofenster mit Angaben zum Programm öffnen.
- **Neuigkeiten** – Öffnet das Fenster News Agent (s. Abschnitt "News Agent" auf S. 198). Dieser Menüpunkt wird angezeigt, wenn ungelesene Neuigkeiten vorliegen.
- **Beenden** – Arbeit von Kaspersky Internet Security beenden (bei Auswahl dieses Menüpunkts wird das Programm aus dem Arbeitsspeicher des Computers entfernt).

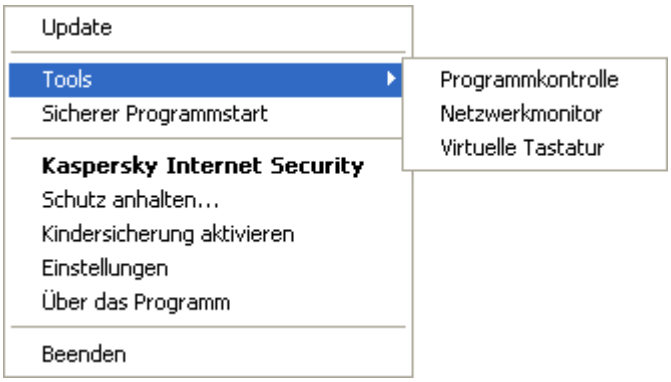

Abbildung 2. Kontextmenü

Wird das Kontextmenü geöffnet, während eine Untersuchungsaufgabe oder Updateaufgabe läuft, so wird ihr Name mit Prozentangabe für das Ausführungsergebnis im Kontextmenü angezeigt. Durch die Auswahl des Menüpunkts mit dem Aufgabennamen gelangen Sie in das Hauptfenster mit einem Bericht über die aktuellen Ausführungsergebnisse.

Um das Kontextmenü zu öffnen,

zeigen Sie im Infobereich der Taskleiste mit der Maus auf das Programmsymbol und führen Sie einen Rechtsklick aus.

Unter dem Betriebssystem Microsoft Windows 7 ist das Programmsymbol standardmäßig ausgeblendet, wobei es für die Arbeit mit dem Programm jedoch eingeblendet werden kann (s. Dokumentation des Betriebssystems).

HAUPTFENSTER VON KASPERSKY INTERNET SECURITY

Die Elemente des Programmhauptfensters bieten Zugriff auf die Hauptfunktionen des Programms.

Das Hauptfenster lässt sich bedingt in drei Bereiche aufteilen:

- Im oberen Fensterbereich befindet sich der Schutzindikator, der den aktuellen Schutzstatus Ihres Computers signalisiert.

Abbildung 3. Aktueller Schutzstatus des Computers

Es gibt drei Varianten für den Schutzstatus. Jeder Status wird durch eine bestimmte Farbe signalisiert. Die Farbe Grün bedeutet, dass der Schutz Ihres Computers dem erforderlichen Niveau entspricht. Gelb und Rot warnen vor unterschiedlichen Sicherheitsrisiken. Als Bedrohung gilt nicht nur der Fund schädlicher Programme,

sondern auch die Verwendung veralteter Datenbanken, die deaktivierten Schutzkomponenten, die Auswahl einer niedrigen Sicherheitsstufe u.a.

Vorhandene Sicherheitsrisiken sollten umgehend behoben werden (s. Abschnitt "Probleme im Computerschutz diagnostizieren und beheben" auf S. 55).

- Die linke Seite des Fensters bietet schnellen Zugriff auf die wichtigsten Programmfunktionen: Schutzkomponenten aktivieren und deaktivieren, Untersuchungsaufgaben und Updateaufgaben für Datenbanken und Programm-Module ausführen, u.a.

Abbildung 4. Linke Seite des Hauptfensters

- Die rechte Seite des Fensters enthält Informationen über die auf der linken Seite ausgewählte Programmfunktion, erlaubt es, die ihre Parameter anzupassen, bietet Werkzeuge zum Ausführen von Aufgaben zur Virensuche, zum Update-Download, u.a.

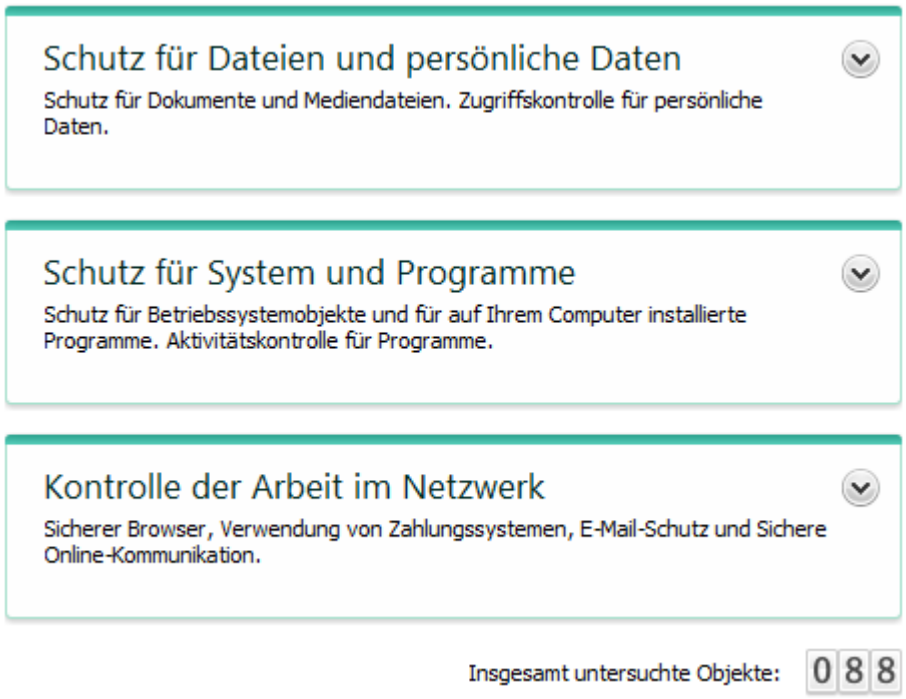
Schutz für Dateien und persönliche Daten
Schutz für Dokumente und Mediendateien. Zugriffskontrolle für persönliche Daten.
Schutz für System und Programme
Schutz für Betriebssystemobjekte und für auf Ihrem Computer installierte Programme. Aktivitätskontrolle für Programme.
Kontrolle der Arbeit im Netzwerk
Sicherer Browser, Verwendung von Zahlungssystemen, E-Mail-Schutz und Sichere Online-Kommunikation.
Insgesamt untersuchte Objekte: 088

Abbildung 5. Rechte Seite des Hauptfensters

Außerdem stehen folgende Schaltflächen und Links zur Verfügung:

- **Einstellungen** – in das Programmkonfigurationsfenster wechseln.
- **Quarantäne** – zur Arbeit mit Objekten, die in die Quarantäne verschoben wurden, wechseln.
- **Berichte** – ermöglicht den Wechsel zum Bericht über die Programmausführung in Form eines Diagramms.
- **Neuigkeiten** – Öffnet das Fenster von News Agent zum Lesen neuer Nachrichten (s. Abschnitt "News Agent" auf S. 198). Der Link erscheint, nachdem das Programm Neuigkeiten empfangen hat.
- **Hilfe** – zum Hilfesystem für Kaspersky Internet Security wechseln.
- **Mein Kaspersky Account** – in den persönlichen Bereich des Benutzers auf der Webseite des technischen Supports gehen (s. Abschnitt "Mein Kaspersky Account" auf S. 206).
- **Support** - Das Fenster mit Informationen über das System und mit Links zu Informationsressourcen von Kaspersky Lab (Webseite des Technischen Supports, Forum) öffnen.
- **Lizenz** – zur Aktivierung von Kaspersky Internet Security bzw. zur Verlängerung der Lizenz wechseln.

Sie können das Aussehen von Kaspersky Internet Security verändern, indem Sie alternative grafische Oberflächen (s. Abschnitt "Aussehen des Programms" auf S. 197) verwenden.

Gehen Sie folgendermaßen vor, um das Programmhauptfenster zu öffnen:

- zeigen Sie im Infobereich der Taskleiste mit der Maus auf das Programmsymbolund führen Sie einen Linksklick aus.

Unter dem Betriebssystem Microsoft Windows 7 ist das Programmsymbol standardmäßig ausgeblendet, wobei es für die Arbeit mit dem Programm jedoch eingeblendet werden kann (s. Dokumentation des Betriebssystems).

- wählen Sie im Kontextmenü den Punkt **Kaspersky Internet Security** (s. Abschnitt "Kontextmenü" auf S. 46);
- Klicken Sie in der Mitte des Kaspersky Gadgets auf das Symbol von Kaspersky Internet Security (nur für die Betriebssysteme Microsoft Windows Vista und Microsoft Windows 7).

MELDUNGSFENSTER UND POPUPMELDUNGEN

Kaspersky Internet Security benachrichtigt Sie mit Hilfe von *Meldungsfenstern* und *Popupmeldungen*, die oberhalb des Programmsymbols im Infobereich der Taskleiste angezeigt werden, über wichtige Ereignisse, die während seiner Ausführung eintreten.

Kaspersky Internet Security zeigt die *Meldungsfenster* immer dann auf dem Bildschirm an, wenn verschiedene Reaktionen auf das Ereignis möglich sind. So können Sie beispielsweise bei Erkennen eines schädlichen Objekts den Zugriff darauf blockieren, dieses löschen oder versuchen, es zu desinfizieren. Das Programm stellt Ihnen die entsprechenden Optionen zu Auswahl. Das Meldungsfenster wird erst dann wieder geschlossen, wenn Sie eine der vorgeschlagenen Optionen ausgewählt haben.

Abbildung 6. Fenster Meldungen

Kaspersky Internet Security zeigt *Popupfenster* auf dem Bildschirm an, um Sie über Ereignisse zu informieren, die keine Entscheidung Ihrerseits über die weitere Vorgehensweise erfordern. Einige Popupmeldungen beinhalten Links, mit deren Hilfe Sie eine vorgeschlagene Aktion ausführen können (z. B. ein Datenbankupdate starten oder zur Programmaktivierung wechseln). Popupmeldungen verschwinden nach kurzer Zeit automatisch vom Bildschirm.

Abbildung 7. Popupmeldung

In Abhängigkeit davon, welche Relevanz das Ereignis für die Computersicherheit besitzt, sind folgende Arten von Meldungen möglich:

- Kritische Meldungen informieren über die Ereignisse, die vorrangige Priorität für die Computersicherheit aufweisen. Beispiele: "Ein schädliches Objekt wurde gefunden" oder "Im System wurde eine gefährliche Aktivität erkannt". Benachrichtigungsfenster und Popupmeldungen dieses Typs werden rot angezeigt.

- Wichtige Meldungen informieren über die Ereignisse, die für die Computersicherheit potentiell wichtig sind. Beispiele: "Ein möglicherweise infiziertes Objekt wurde gefunden" oder "Im System wurde verdächtige Aktivität erkannt". Benachrichtigungsfenster und Popupmeldungen dieses Typs werden gelb angezeigt.

- Informative Meldungen informieren über die Ereignisse, die vom Standpunkt der Sicherheit aus keine vorrangige Priorität besitzen. Benachrichtigungsfenster und Popupmeldungen dieses Typs werden grün angezeigt.

PROGRAMMKONFIGURATIONSFENSTER

Das Konfigurationsfenster von Kaspersky Internet Security dient dazu, die allgemeinen Programmfunktionen, einzelne Schutzkomponenten, Untersuchungs- und Update-Aufgaben anzupassen. Außerdem sind hier erweiterte Einstellungen für andere Aufgaben möglich (s. Abschnitt "Erweiterte Programmeinstellungen" auf S. 81).

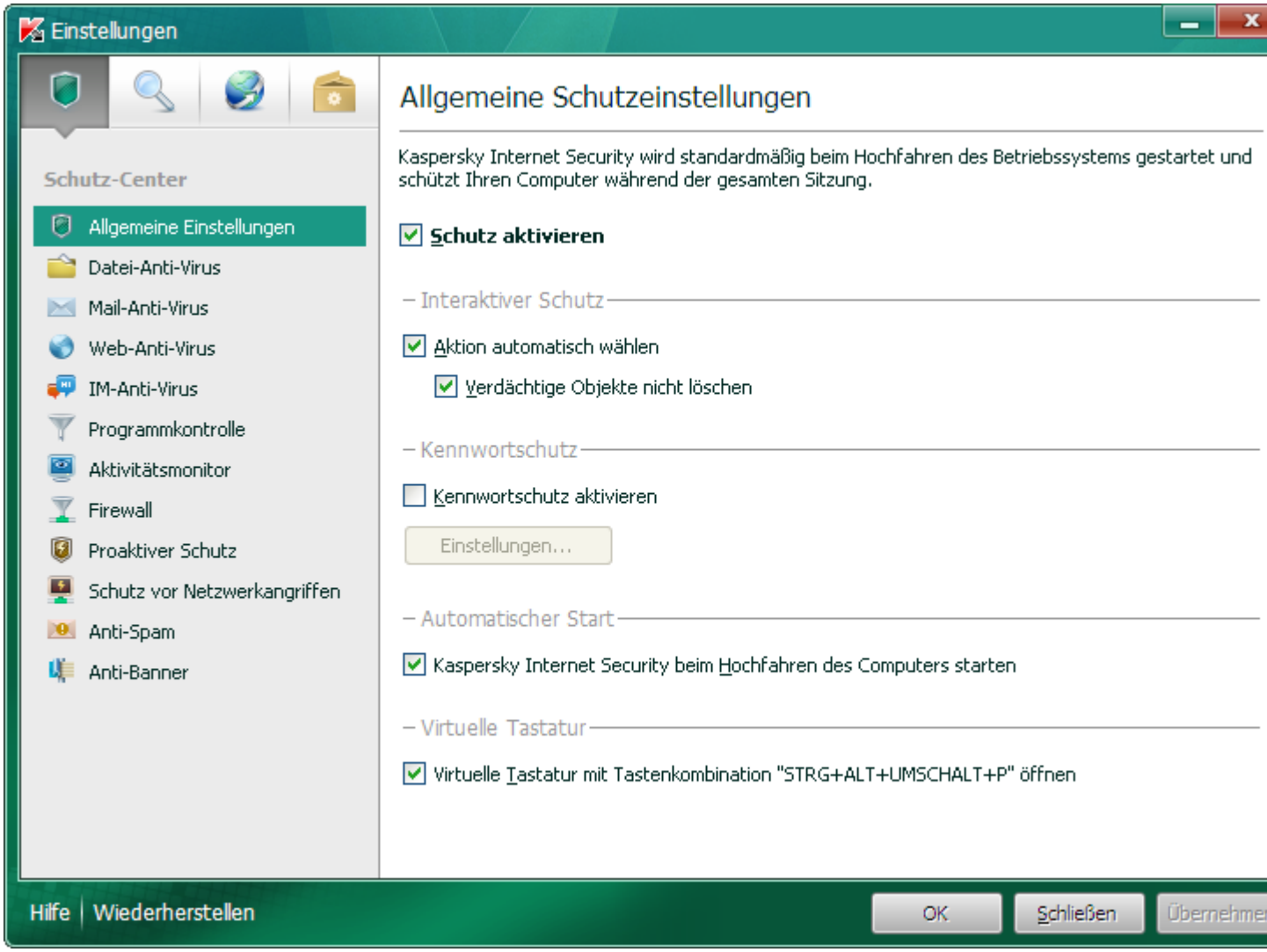

Abbildung 8. Programmkonfigurationsfenster

Das Konfigurationsfenster besteht aus zwei Teilen:

- Im linken Bereich kann eine Programmkomponente, eine Aufgabe oder ein anderes Element gewählt werden, die/das angepasst werden soll.
- Die rechte Fensterseite enthält Steuerelemente, mit denen ein im linken Bereich gewähltes Element angepasst werden kann.

Komponenten, Aufgaben und andere Elemente sind auf der linken Fensterseite in folgende Abschnitte untergliedert:

– **Schutz-Center**

– **Untersuchung des Computers**

– **Update**.

– **Erweiterte Einstellungen**.

Gehen Sie folgendermaßen vor, um das Konfigurationsfenster zu öffnen:

- Verwenden Sie im oberen Bereich des Programmhauptfensters den Link **Einstellungen** (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47);
- wählen Sie im Kontextmenü den Punkt **Einstellungen** (s. Abschnitt "Kontextmenü" auf S. 46);
- klicken Sie im Interface von Kaspersky Gadget auf die Schaltfläche mit dem Symbol **Einstellungen** (nur für die Betriebssysteme Microsoft Windows Vista und Microsoft Windows 7). Dieser Schaltfläche muss mit der Funktion zum Öffnen des Konfigurationsfensters belegt sein (s. Abschnitt "Wie das Kaspersky Gadget verwendet wird" auf S. 78).

Zur Auswahl des erforderlichen Abschnitts im Konfigurationsfenster,

klicken Sie auf das Symbol des entsprechenden Abschnitts im linken oberen Bereich des Fensters (s. Abbildung oben).

KASPERSKY GADGET

Wenn Kaspersky Internet Security auf einem Computer mit dem Betriebssystem Microsoft Windows Vista oder Microsoft Windows 7 eingesetzt wird, steht das Kaspersky Gadget zur Verfügung (weiter auch einfach als *Gadget* bezeichnet).

Kaspersky Gadget bietet schnellen Zugriff auf die Grundfunktionen des Programms: Schutzstatus des Computers anzeigen, Objekte auf Viren untersuchen, Berichte über die Programmarbeit anzeigen, u.a.

Nach der Installation von Kaspersky Internet Security auf einem Computer mit dem Betriebssystem Microsoft Windows 7 erscheint das Gadget automatisch auf dem Desktop. Wenn das Programm auf einem Computer mit dem Betriebssystem Microsoft Windows Vista installiert wird, muss das Gadget manuell zur Sidebar von Microsoft Windows hinzugefügt werden (s. Dokumentation des Betriebssystems).

Abbildung 9. Kaspersky Gadget

PROGRAMM STARTEN UND BEENDEN

Kaspersky Internet Security wird nach der Installation automatisch gestartet. In der Grundeinstellung ist vorgesehen, dass das Programm künftig beim Hochfahren des Betriebssystems automatisch gestartet wird.

IN DIESEM ABSCHNITT

Automatischen Start aktivieren und deaktivieren 54

Programm manuell starten und beenden 54

AUTOMATISCHEN START AKTIVIEREN UND DEAKTIVIEREN

Unter automatischem Programmstart wird hier der Start von Kaspersky Internet Security verstanden, der ohne Ihr Zutun sofort nach dem Hochfahren des Betriebssystems ausgeführt wird. Diese Startvariante gilt als Standard.

Geben Sie folgendermaßen vor, um den automatischen Start des Programms zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** den Abschnitt **Allgemeine Einstellungen**.
3. Deaktivieren Sie auf der rechten Fensterseite im Block **Autostart** das Kontrollkästchen **Kaspersky Internet Security beim Hochfahren des Computers starten**, um den automatischen Programmstart auszuschalten. Aktivieren Sie das Kontrollkästchen, um den automatischen Start des Programms einzuschalten:

PROGRAMM MANUELL STARTEN UND BEENDEN

Kaspersky Lab warnt davor, Kaspersky Internet Security zu beenden, da andernfalls der Computer und Ihre persönlichen Daten bedroht sind. Sollte es trotzdem notwendig sein, so wird empfohlen, den Computerschutz nur anzuhalten, ohne das Programm zu beenden.

Kaspersky Internet Security muss manuell gestartet werden, falls Sie den automatischen Programmstart verwenden (s. Abschnitt "Automatischen Start aktivieren und deaktivieren" auf S. 54).

Um das Programm manuell zu starten,

gehen Sie im **Start** auf **Programme** → **Kaspersky Internet Security 2011** → **Kaspersky Internet Security 2011**.

Um die Arbeit des Programms zu beenden,

öffnen Sie durch Rechtsklick das Kontextmenü des Programmsymbols, das sich im Infobereich der Taskleiste befindet, und wählen Sie den Punkt **Beenden**.

Unter dem Betriebssystem Microsoft Windows 7 ist das Programmsymbol standardmäßig ausgeblendet, wobei es für die Arbeit mit dem Programm jedoch eingeblendet werden kann (s. Dokumentation des Betriebssystems).

SCHUTZSTATUS DES COMPUTERS

Dieser Abschnitt informiert darüber, wie ermittelt wird, ob der Computer im Augenblick sicher ist oder ob seine Sicherheit bedroht ist. Außerdem wird die Neutralisierung von vorhandenen Bedrohungen beschrieben. Hier finden Sie Informationen darüber, wie der Schutz während der Arbeit von Kaspersky Internet Security aktiviert, deaktiviert und vorübergehend angehalten werden kann.

IN DIESEM ABSCHNITT

Probleme im Computerschutz diagnostizieren und beheben 55

Schutz aktivieren und deaktivieren 57

Schutz anhalten und fortsetzen 58

PROBLEME IM COMPUTERSCHUTZ DIAGNOSTIZIEREN UND BEHEBEN

Probleme beim Schutz des Computers werden durch den Schutzindikator signalisiert, der sich im oberen Bereich des Programmhauptfensters befindet (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47). Der Indikator ändert seine Farbe in Abhängigkeit vom Schutzstatus des Computers: Die Farbe Grün bedeutet, dass der Computer sicher ist. Gelb signalisiert, dass der Schutz Probleme aufweist, und Rot warnt vor einer ernsthaften Bedrohung für die Computersicherheit. Probleme und Sicherheitsrisiken sollten umgehend behoben werden.

Durch Klick auf das Indikatorsymbol im Programmhauptfenster kann das Fenster **Schutzstatus** geöffnet werden (s. Abb. unten). Es enthält ausführliche Angaben zum Schutzstatus des Computers und bietet Aktionsvarianten zum Beheben von Problemen und Gefahren.

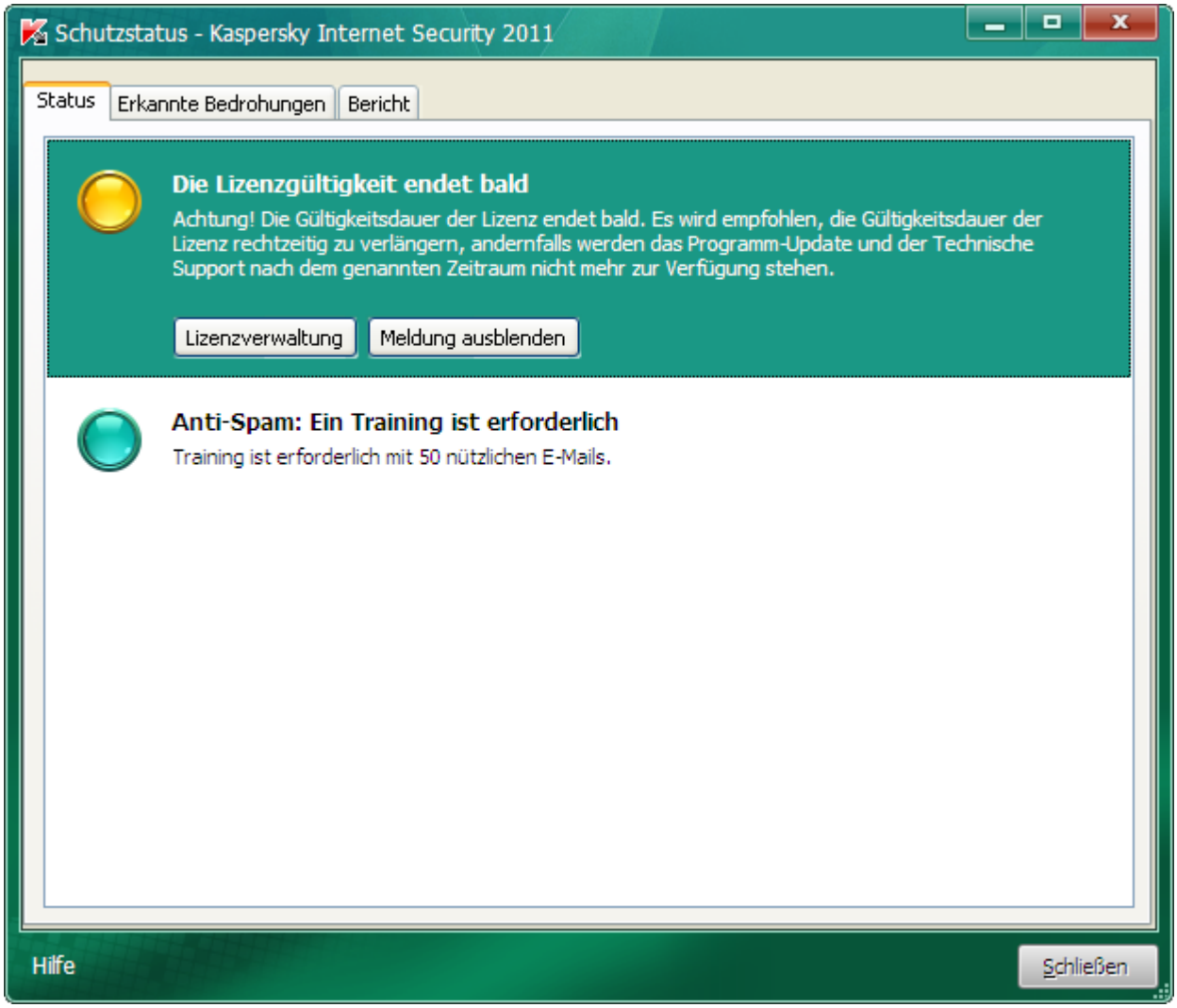
Schutzstatus - Kaspersky Internet Security 2011
Status
Erkannte Bedrohungen
Bericht
Die Lizenzgültigkeit endet bald
Achtung! Die Gültigkeitsdauer der Lizenz endet bald. Es wird empfohlen, die Gültigkeitsdauer der Lizenz rechtzeitig zu verlängern, andernfalls werden das Programm-Update und der Technische Support nach dem genannten Zeitraum nicht mehr zur Verfügung stehen.
Lizenzverwaltung
Meldung ausblenden
Anti-Spam: Ein Training ist erforderlich
Training ist erforderlich mit 50 nützlichen E-Mails.
Hilfe
Schließen

Abbildung 10. Sicherheitsprobleme beheben

Die Registerkarte **Status** im Fenster **Schutzstatus** enthält eine Liste der im Schutz vorhandenen Probleme. Dazu zählen auch Probleme, die auf Abweichungen von der optimalen Programmfunktion zurückgehen (z.B. veraltete Datenbanken). Zum Beheben von Gefahren werden Aktionsvarianten angeboten:

- Sofort beheben. Mit Hilfe der entsprechenden Schaltflächen können Sie direkt zur sofortigen Neutralisierung der Probleme übergehen. Diese Aktion gilt als empfohlen.

- Behebung aufschieben. Wenn das sofortige Beheben eines Problems aufgrund bestimmter Umstände nicht möglich ist, kann diese Aktion aufgeschoben werden und Sie können später dazu zurückkehren. Klicken Sie dazu auf **Meldung ausblenden**.

  Beachten Sie, dass es für kritische Probleme nicht vorgesehen ist, das Beheben aufzuschieben. Zu diesen Problemen gehören beispielsweise die Existenz nicht neutralisierter schädlicher Objekte, Funktionsstörungen einer oder mehrerer Komponenten und beschädigte Programmdateien.

Um Meldungen, die zuvor ausgeblendet wurden, erneut in der allgemeinen Liste anzuzeigen, aktivieren Sie das Kontrollkästchen **Ausgeblendete Meldungen anzeigen**. Dieses Kontrollkästchen befindet sich im unteren Bereich der Registerkarte, falls ausgeblendete Meldungen vorhanden sind.

Auf der Registerkarte **Erkannte Bedrohungen** können Sie eine Liste der gefundenen schädlichen und möglicherweise schädlichen Objekte ansehen und eine Aktion für diese Objekte wählen (z.B. in die Quarantäne verschieben). Zur Auswahl einer Aktion dienen die über der Liste angebrachten Steuerelemente sowie das Kontextmenü für die Listeneinträge.

Auf der Registerkarte **Bericht** können die Berichte über die Programmarbeit überprüft werden (s. Abschnitt "Aufrufen des Berichts über die Programmaktivität" auf S. 76).

SCHUTZ AKTIVIEREN UND DEAKTIVIEREN

Kaspersky Internet Security wird in der Grundeinstellung automatisch beim Start des Betriebssystems gestartet und schützt Ihren Computer während der gesamten Sitzung. Alle Schutzkomponenten sind aktiv.

Sie können den Schutz, der von Kaspersky Internet Security gewährleistet wird, vollständig oder teilweise deaktivieren.

Die Kaspersky-Lab-Spezialisten warnen ausdrücklich davor, den Schutz zu deaktivieren, weil dies zur Infektion Ihres Computers und zu Datenverlust führen kann. Sollte dies tatsächlich notwendig sein, so wird empfohlen, den Schutz vorübergehend anzuhalten (s. Abschnitt "Schutz anhalten und fortsetzen" auf S. 58).

Wenn der Schutz deaktiviert wird, wird die Arbeit aller Komponenten beendet.

Darüber informieren folgende Merkmale:

- inaktives (graues) Programmsymbol im Infobereich der Taskleiste (s. Abschnitt "Symbol im Infobereich der Taskleiste" auf S. 45).
- rote Farbe des Sicherheitsindikators im oberen Bereich des Programmhauptfensters.

Beachten Sie, dass der Schutz hier ausdrücklich im Kontext der Schutzkomponenten beschrieben wird. Das Deaktivieren oder Anhalten von Schutzkomponenten übt keinen Einfluss auf die Ausführung von Aufgaben zur Virensuche und zum Update für Kaspersky Internet Security aus.

Der Schutz kann vom Programmkonfigurationsfenster aus vollständig aktiviert oder deaktiviert werden (s. Abschnitt "Programmkonfigurationsfenster" auf S. 52). Die einzelnen Programmkomponenten können vom Konfigurationsfenster oder vom Programmhauptfenster aus aktiviert oder deaktiviert werden (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47).

Gehen Sie folgendermaßen vor, um den Schutz vollständig zu deaktivieren oder zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** den Abschnitt **Allgemeine Einstellungen**.
3. Deaktivieren Sie das Kontrollkästchen **Schutz aktivieren**, um den Schutz auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um den Schutz einzuschalten.

Gehen Sie folgendermaßen vor, um eine Schutzkomponente vom Konfigurationsfenster aus zu deaktivieren oder zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente, die aktiviert oder deaktiviert werden soll.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **<Name der Komponente> aktivieren**, um die Komponente auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um die Komponente einzuschalten.

Gehen Sie folgendermaßen vor, um eine Schutzkomponente vom Programmhauptfenster aus zu deaktivieren oder zu aktivieren:

1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Schutz-Center** aus.

2. Öffnen Sie auf der rechten Fensterseite durch Linksklick den Block, zu dem die Komponente gehört, die aktiviert oder deaktiviert werden soll.

3. Klicken Sie auf die Schaltfläche mit dem Namen der Komponente, um das Menü zur Aktionsauswahl zu öffnen. Wählen Sie in diesem Menü den Punkt **<Name der Komponente> aktivieren**, um die Komponente einzuschalten, oder den Punkt **<Name der Komponente> deaktivieren**, um die Komponente auszuschalten.

   Wird eine Komponente aktiviert, so wird das Symbol links von ihrem Namen grün, wird sie deaktiviert, so wird das Symbol grau.

SCHUTZ ANHALTEN UND FORTSETZEN

Das Anhalten des Schutzes bedeutet, dass alle Komponenten für einen bestimmten Zeitraum ausgeschaltet werden.

Darüber informieren folgende Merkmale:

- inaktives (graues) Programmsymbol im Infobereich der Taskleiste (s. Abschnitt "Symbol im Infobereich der Taskleiste" auf S. 45).

- rote Farbe des Sicherheitsindikators im oberen Bereich des Programmhauptfensters.

Beachten Sie, dass der Schutz hier ausdrücklich im Kontext der Schutzkomponenten beschrieben wird. Das Deaktivieren oder Anhalten von Schutzkomponenten übt keinen Einfluss auf die Ausführung von Aufgaben zur Virensuche und zum Update für Kaspersky Internet Security aus.

Wenn im Augenblick, als der Schutz beendet wurde, auf dem Computer Netzwerkverbindungen vorhanden waren, erscheint auf dem Bildschirm eine Meldung darüber, dass diese Verbindungen getrennt werden.

Bei der Arbeit auf einem Computer mit dem Betriebssystem Microsoft Windows Vista oder Microsoft Windows 7 kann der Schutz mit Hilfe des Kaspersky Gadgets angehalten werden. Dafür muss eine der Schaltflächen des Kaspersky Gadgets mit der Funktion zum Anhalten des Schutzes belegt sein (s. Abschnitt "Wie das Kaspersky Gadget verwendet wird" auf S. 78).

Gehen Sie folgendermaßen vor, um den Computerschutz anzuhalten:

1. Verwenden Sie eine der folgenden Methoden, um das Fenster **Schutz anhalten** zu öffnen:

   - wählen Sie im Kontextmenü des Programmsymbols den Punkt **Schutz anhalten** (s. Abschnitt "Kontextmenü" auf S. 46).

   - klicken Sie im Interface von Kaspersky Gadget auf die Schaltfläche mit dem Symbol **Schutz anhalten** (nur für die Betriebssysteme Microsoft Windows Vista und Microsoft Windows 7).

2. Wählen Sie im Fenster **Schutz anhalten** den Zeitraum, nach dem der Schutz wieder aktiviert werden soll:

   - **Anhalten für** – Der Schutz wird nach Ablauf des unten festgelegten Zeitraums wieder aktiviert.

   - **Anhalten bis zum Neustart** – Der Schutz wird nach dem Neustart des Programms oder des Systems aktiviert (unter der Bedingung, dass der automatische Programmstart aktiviert ist (s. Abschnitt "Automatischen Start aktivieren und deaktivieren"auf S. 54)).

   - **Anhalten** – Der Schutz wird erst dann wieder aktiviert, wenn Sie ihn fortsetzen (s. unten).

- *Um den Computerschutz fortzusetzen,*

  wählen Sie im Kontextmenü des Programmsymbols den Punkt **Schutz fortsetzen** (s. Abschnitt "Kontextmenü" auf S. 46).

Der Computerschutz kann auf diese Weise fortgesetzt werden, wenn die Variante **Anhalten**, **Zum festgelegten Zeitpunkt anhalten** oder **Anhalten bis zum Neustart** gewählt wurde.

LÖSUNGEN FÜR TYPISCHE AUFGABEN

Dieser Abschnitt bietet eine Anleitung für die grundlegenden Augaben des Programms, die der Benutzer am häufigsten benötigt.

IN DIESEM ABSCHNITT

Wie das Programm aktiviert wird. ... 60

Lizenzerwerb oder -verlängerung ... 61

Was tun, wenn das Programm Meldungen anzeigt? ... 62

Aktualisierung von Programmdatenbanken und -modulen ... 62

Wie wichtige Computerbereiche auf Viren untersucht werden. ... 63

Untersuchung von Dateien, Ordnern, Laufwerken und anderen Objekten auf Viren ... 64

Wie eine vollständige Virenuntersuchung des Computers ausgeführt wird. ... 65

Wie der Computer auf Schwachstellen untersucht wird. ... 66

Wie Ihre persönlichen Daten vor Diebstahl geschützt werden. ... 67

Was tun, wenn Sie vermuten, dass ein Objekt von einem Virus infiziert ist? ... 69

Wie mit einer großen Anzahl von Spam-Mails verfahren wird? ... 70

Was tun, wenn Sie vermuten, dass Ihr Computer infiziert ist? ... 71

Wie ein Objekt wiederhergestellt wird, das vom Programm gelöscht oder desinfiziert wurde. ... 72

Wie eine Notfall-CD erstellt und verwendet wird. ... 73

Aufrufen des Berichts über die Programmaktivität ... 76

Wie die Standardeinstellungen des Programms wiederhergestellt werden ... 76

Wie Programmeinstellungen von Kaspersky Internet Security auf einen anderen Computer übertragen werden. ... 78

Wie das Kaspersky Gadget verwendet wird. ... 78

WIE WIRD DAS PROGRAMM AKTIVIERT?

Durch die *Aktivierung* erlangt die Lizenz für die Nutzung der Vollversion des Programms ihre Gültigkeit für den entsprechenden Zeitraum.

Wenn Sie das Programm nicht im Verlauf der Installation aktiviert haben, können Sie dies später nachholen. Falls eine Programmaktivierung notwendig ist, werden Sie von Kaspersky Internet Security durch entsprechende Meldungen im Infobereich der Taskleiste daran erinnert.

Gehen Sie folgendermaßen vor, um den Aktivierungsassistenten für Kaspersky Internet Security zu starten:

- Verwenden Sie im Meldungsfenster von Kaspersky Internet Security, das im Infobereich der Taskleiste erscheint, auf den Link **Bitte aktivieren Sie das Programm**.

- Verwenden Sie im unteren Bereich des Programmhauptfensters den Link **Lizenz**. Klicken Sie im folgenden Fenster **Lizenzen verwalten** auf **Programm mit neuer Lizenz aktivieren**.

Details zu den einzelnen Schritte des Assistenten:

Schritt 1. Lizenztyp wählen und Aktivierungscode eingeben

Vergewissern Sie sich, dass im Assistentenfenster die Variante **Kommerzielle Version aktivieren** gewählt wurde, geben Sie den Aktivierungscode (s. Abschnitt "Über den Aktivierungscode" auf S. 43) im entsprechenden Feld ein und klicken Sie auf **Weiter**.

Schritt 2. Aktivierungsanfrage

Im ersten Schritt sendet der Assistent eine Anfrage zur Aktivierung der kommerziellen Programmversion an den Aktivierungsserver. Der Assistent geht nach erfolgreicher Anfrage automatisch zum nächsten Schritt.

Schritt 3. Anmeldedaten eingeben

Eine Anmeldung ist erforderlich, damit sich der Benutzer künftig an den Technischen Support wenden kann. Nicht registrierte Benutzer werden hier kurz aufgehalten.

Geben Sie Ihre Anmeldedaten an und klicken Sie dann auf **Weiter**.

Schritt 4. Aktivierung

In diesem Schritt stellt der Assistent eine Verbindung mit dem Aktivierungsserver her, um die Programmaktivierung und die Registrierung des Benutzers abzuschließen, woraufhin der Assistent automatisch zum nächsten Fenster wechselt.

Schritt 5. Assistent abschließen

Dieses Fenster des Assistenten informiert über die Aktivierungsergebnisse: Typ und Gültigkeitsdauer der verwendeten Lizenz.

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

LIZENZERWERB ODER -VERLÄNGERUNG

Wenn Sie Kaspersky Internet Security installiert haben und keine Lizenz besitzen, können Sie die Lizenz nach der Programminstallation erwerben. Wenn die Gültigkeit einer Lizenz bald abläuft, können Sie diese verlängern. Sie erhalten einen Aktivierungscode, mit dem das Programm aktiviert werden muss (s. Abschnitt "Wie wird das Programm aktiviert?" auf S. 60).

Gehen Sie folgendermaßen vor, um eine Lizenz zu erwerben:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im unteren Fensterbereich auf **Lizenz kaufen**.

   Die Webseite des Online-Shops wird geöffnet. Dort können Sie eine Lizenz erwerben.

Gehen Sie folgendermaßen vor, um die Gültigkeitsdauer einer Lizenz zu verlängern:

1. Öffnen Sie das Programmhauptfenster und klicken Sie unten im Hauptfenster auf den Link **Lizenz**.

   Das Fenster **Lizenzen verwalten** wird geöffnet.

2. Klicken Sie auf die Schaltfläche **Gültigkeitsdauer der Lizenz verlängern**.

   Eine Webseite zur Lizenzaktualisierung wird geöffnet. Dort können Sie die Gültigkeitsdauer Ihrer Lizenz verlängern.

WAS TUN, WENN DAS PROGRAMM MELDUNGEN ANZEIGT?

Meldungen, die das Programm im Infobereich der Taskleiste anzeigt, informieren über Ereignisse bei der Arbeit des Programms und erfordern Ihre Aufmerksamkeit. In Abhängigkeit von der Priorität eines Ereignisses sind folgende Arten von Meldungen möglich:

- Kritische Meldungen informieren über die Ereignisse, die vorrangige Priorität für die Computersicherheit aufweisen. Beispiele: "Ein schädliches Objekt wurde gefunden" oder "Im System wurde eine gefährliche Aktivität erkannt". Benachrichtigungsfenster und Popupmeldungen dieses Typs werden rot angezeigt.

- Wichtige Meldungen informieren über die Ereignisse, die für die Computersicherheit potentiell wichtig sind. Beispiele: "Ein möglicherweise infiziertes Objekt wurde gefunden" oder "Im System wurde verdächtige Aktivität erkannt". Benachrichtigungsfenster und Popupmeldungen dieses Typs werden gelb angezeigt.

- Informative Meldungen informieren über die Ereignisse, die vom Standpunkt der Sicherheit aus keine vorrangige Priorität besitzen. Benachrichtigungsfenster und Popupmeldungen dieses Typs werden grün angezeigt.

Erscheint eine solche Benachrichtigung auf dem Bildschirm, muss eine der vorgegebenen Varianten für die weitere Vorgehensweise ausgewählt werden. Als optimal gilt die von Kaspersky Lab empfohlene Variante.

AKTUALISIERUNG VON PROGRAMMDATENBANKEN UND -MODULEN

Kaspersky Internet Security überprüft in der Grundeinstellung automatisch, ob auf den Kaspersky-Lab-Updateservern neue Updates vorhanden sind. Wenn auf dem Server neue Updates vorhanden sind, führt Kaspersky Internet Security im Hintergrundmodus den Download und die Installation der Updates durch. Sie können das Update von Kaspersky Internet Security jederzeit starten.

Um Updates von den Kaspersky-Lab-Servern herunterzuladen, ist eine Internetverbindung erforderlich.

Um das Update aus dem Kontextmenü zu starten,

wählen Sie im Kontextmenü des Programmsymbols den Punkt **Update**.

Gehen Sie folgendermaßen vor, um das Update aus dem Hauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Update**.

2. Klicken Sie auf der rechten Fensterseite auf den Block **Update ausführen**.

   Die Informationen über das laufende Update werden angezeigt:

   - im Abschnitt **Update** des Hauptfensters des Programms, im Block **Das Update wird ausgeführt**.

- im Fenster **Update**, das mit der Schaltfläche **Das Update wird ausgeführt** geöffnet wird.
- im Kontextmenü des Programmsymbols..

Gehen Sie folgendermaßen vor, um das Update anzuhalten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Update**.
2. Klicken Sie auf der rechten Fensterseite auf **Das Update wird ausgeführt**.
3. Klicken Sie im folgenden Fenster **Update** auf **Stopp**.
4. Klicken Sie im Bestätigungsfenster auf **Ja**.

WIE WICHTIGE COMPUTERBEREICHE AUF VIREN UNTERSUCHT WERDEN.

Unter der Untersuchung wichtiger Bereiche ist die Untersuchung von Objekten zu verstehen, die während des Hochfahrens des Betriebssystems geladen werden, die Untersuchung des Arbeitsspeichers, der Bootsektoren der Festplatte und der vom Benutzer hinzugefügten Objekte (s. Abschnitt "Liste der Untersuchungsobjekte erstellen" auf S. 87).

Sie können die Untersuchung der wichtigen Bereiche auf folgende Weise starten:

- mit einer zuvor hergestellten Verknüpfung (s. S. 91).
- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47)

Gehen Sie folgendermaßen vor, um die Untersuchung mit Hilfe einer Verknüpfung zu starten:

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und öffnen Sie den Ordner, in dem Sie die Verknüpfung erstellt haben.
2. Starten Sie die Untersuchung durch Doppelklick auf die Verknüpfung.

   Die Informationen über die laufende Untersuchung werden angezeigt:

   - im Abschnitt **Untersuchung** des Hauptfensters des Programms, im Block **Untersuchung wichtiger Bereiche wird ausgeführt**;
   - im Fenster **Untersuchung wichtiger Bereiche** , das mit der Schaltfläche **Untersuchung wichtiger Bereiche wird ausgeführt** geöffnet wird.
   - im Kontextmenü des Programmsymbols..

Gehen Sie folgendermaßen vor, um die Untersuchung aus dem Programmhauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.
2. Klicken Sie auf der rechten Seite des Hauptfensters auf **Untersuchung wichtiger Bereiche ausführen**.

   Die Informationen über die laufende Untersuchung werden angezeigt:

   - im Abschnitt **Untersuchung** des Hauptfensters des Programms, im Block **Untersuchung wichtiger Bereiche wird ausgeführt**;

- im Fenster **Untersuchung wichtiger Bereiche** , das mit der Schaltfläche **Untersuchung wichtiger Bereiche wird ausgeführt** geöffnet wird.

- im Kontextmenü des Programmsymbols..

Gehen Sie folgendermaßen vor, um die Untersuchung wichtiger Bereiche anzuhalten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.

2. Klicken Sie auf der rechten Seite des Fensters auf den Block **Untersuchung wichtiger Bereiche wird ausgeführt**.

3. Klicken Sie im folgenden Fenster **Untersuchung wichtiger Bereiche** auf **Stopp**.

4. Klicken Sie im Bestätigungsfenster auf **Ja**.

UNTERSUCHUNG VON DATEIEN, ORDNERN, LAUFWERKEN UND ANDEREN OBJEKTEN AUF VIREN

Ein bestimmtes Objekt kann folgendermaßen auf Viren untersucht werden:

- mit Hilfe des Kontextmenüs für ein Objekt

- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47)

- mit Hilfe des Gadgets von Kaspersky Internet Security (nur für die Betriebssysteme Microsoft Windows Vista und Microsoft Windows 7).

Gehen Sie folgendermaßen vor, um eine Untersuchungsaufgabe aus dem Kontextmenü eines Objekts zu starten:

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und gehen Sie in den Ordner, in dem sich das Untersuchungsobjekt befindet.

2. Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt (s. Abb. unten) und wählen Sie den Punkt **Auf Viren untersuchen**.

   Der Vorgang und das Ergebnis der Aufgabenausführung werden im folgenden Fenster **Auf Viren untersuchen** angezeigt.

Abbildung 11. Kontextmenü für ein Objekt in Microsoft Windows

Gehen Sie folgendermaßen vor, um die Untersuchung eines Objekts aus dem Programmhauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.

2. Verwenden Sie eine der folgenden Methoden, um ein Untersuchungsobjekt anzugeben:

   - Öffnen Sie mit dem Link **wählen**, der sich auf der rechten Fensterseite befindet, das Fenster **Untersuchung von Objekten** und aktivieren Sie die Kontrollkästchen für die Ordner und Laufwerke, die untersucht werden sollen. Wenn die zu untersuchenden Objekte nicht in diesem Fenster enthalten sind, öffnen Sie mit dem Link **Hinzufügen** das Fenster **Untersuchungsobjekt wählen** und wählen Sie die Untersuchungsobjekte.

   - Ziehen Sie ein Untersuchungsobjekt mit der Maus in den dafür vorgesehenen Bereich des Hauptfensters (s. Abb. unten).

   Der Vorgang der Aufgabenausführung wird im folgenden Fenster **Auf Viren untersuchen** angezeigt.

Abbildung 12. Fensterbereich, in den ein Untersuchungsobjekt gezogen werden muss

Um ein Objekt mit Hilfe des Gadgets auf Viren zu untersuchen,

ziehen Sie das Untersuchungsobjekt auf das Gadget.

Der Vorgang der Aufgabenausführung wird im folgenden Fenster **Auf Viren untersuchen** angezeigt.

Gehen Sie folgendermaßen vor, um die Objektuntersuchung anzuhalten:

1. Klicken Sie im Fenster **Auf Viren untersuchen**, das sich nach Start der Objektuntersuchung öffnet, auf **Stopp** oder schließen Sie das Fenster.

2. Klicken Sie im erscheinenden Bestätigungsfenster zum Anhalten der Untersuchung auf **Ja**.

WIE EINE VOLLSTÄNDIGE VIRENUNTERSUCHUNG DES COMPUTERS AUSGEFÜHRT WIRD.

Eine vollständige Virenuntersuchung kann folgendermaßen gestartet werden:

- mit einer zuvor hergestellten Verknüpfung (s. S. 91).

- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47)

Gehen Sie folgendermaßen vor, um die vollständige Untersuchung mit Hilfe einer Verknüpfung zu starten:

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und öffnen Sie den Ordner, in dem Sie die Verknüpfung erstellt haben.

2. Starten Sie die Untersuchung durch Doppelklick auf die Verknüpfung.

   Die Informationen über die laufende Untersuchung werden angezeigt:

- im Abschnitt **Untersuchung** des Hauptfensters des Programms, im Block **Vollständige Untersuchung wird ausgeführt**;
- im Fenster **Vollständige Untersuchung**, das sich beim Anklicken des Blocks **Vollständige Untersuchung wird ausgeführt** öffnet;
- im Kontextmenü des Programmsymbols..

Gehen Sie folgendermaßen vor, um die vollständige Untersuchung aus dem Programmhauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.
2. Klicken Sie auf der rechten Fensterseite auf **Vollständige Untersuchung ausführen**.

   Die Informationen über die laufende Untersuchung werden angezeigt:

   - im Abschnitt **Untersuchung** des Hauptfensters des Programms, im Block **Vollständige Untersuchung wird ausgeführt**;
   - im Fenster **Vollständige Untersuchung**, das sich beim Anklicken des Blocks **Vollständige Untersuchung wird ausgeführt** öffnet;
   - im Kontextmenü des Programmsymbols..

Gehen Sie wie folgt vor, um die vollständige Untersuchung anzuhalten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.
2. Klicken Sie auf der rechten Fensterseite auf **Vollständige Untersuchung wird ausgeführt**.
3. Klicken Sie im folgenden Fenster **Vollständige Untersuchung** auf **Stopp**.
4. Klicken Sie im Bestätigungsfenster auf **Ja**.

WIE DER COMPUTER AUF SCHWACHSTELLEN UNTERSUCHT WIRD.

Schwachstellen sind Teile eines Programmcodes, den Angreifer für ihre Ziele nutzen können, um beispielsweise Daten zu kopieren, die von Programmen mit ungeschütztem Code verwendet werden. Die Untersuchung Ihres Computers auf potentielle Schwachstellen erlaubt es, solche "Schwachpunkte" im Schutz des Rechners zu finden. Erkannte Schwachstellen sollten beseitigt werden.

Sie können die Schwachstellensuche auf folgende Weise starten:

- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47)
- mit Hilfe einer zuvor erstellten Verknüpfung

Gehen Sie folgendermaßen vor, um die Aufgabe mit Hilfe einer Verknüpfung zu starten:

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und öffnen Sie den Ordner, in dem Sie die Verknüpfung erstellt haben.
2. Starten Sie die Aufgabe zur Schwachstellensuche durch Doppelklick auf die Verknüpfung.

   Informationen über die Aufgabenausführung werden im geöffneten Fenster **Schwachstellensuche** angezeigt.

Gehen Sie folgendermaßen vor, um die Aufgabe aus dem Programmhauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Tools**.
2. Klicken Sie auf der rechten Fensterseite auf **Schwachstellensuche im System**.

   Informationen über die Aufgabenausführung werden im geöffneten Fenster **Schwachstellensuche** angezeigt.

Gehen Sie folgendermaßen vor, um die Schwachstellensuche anzuhalten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Tools**.
2. Klicken Sie auf der rechten Fensterseite auf **Schwachstellensuche im System**.
3. Klicken Sie im folgenden Fenster **Schwachstellensuche** auf **Stopp**.
4. Klicken Sie im Bestätigungsfenster zum Anhalten der Schwachstellensuche auf **Ja**.

WIE IHRE PERSÖNLICHEN DATEN VOR DIEBSTAHL GESCHÜTZT WERDEN.

Mit Kaspersky Internet Security können Sie Ihre persönlichen Daten vor Diebstahl schützen. Zu diesen zählen beispielsweise:

- Kennwörter, Benutzernamen und andere Anmeldedaten
- Konto- und Kreditkartennummern

Kaspersky Internet Security enthält Komponenten und Tools, mit denen Ihre persönlichen Daten vor Diebstahl geschützt werden können, wenn Angreifer Methoden wie Phishing und das Abfangen von Daten, die über die Tastatur eingegeben werden, einsetzen.

Für den Schutz vor Phishing ist Anti-Phishing verantwortlich, das zu den Komponenten Web-Anti-Virus, Anti-Spam und IM-Anti-Virus gehört.

Für den Schutz vor dem Abfangen von Daten, die über die Tastatur eingegeben werden, dient die *Virtuelle Tastatur*.

IN DIESEM ABSCHNITT

Schutz vor Phishing 67

Virtuelle Tastatur 68

SCHUTZ VOR PHISHING

Phishing ist eine Art des Internetbetrugs, bei der Kreditkartennummern, PIN-Codes und andere persönliche Daten "geangelt" werden, um Geld zu stehlen.

Phishing ist häufig mit Online-Banking verbunden. Die Angreifer erstellen eine exakte Kopie der Homepage einer bestimmten Bank und schreiben die Kunden im Namen der Bank Briefe an. Den Kunden wird mitgeteilt, im Online-Banking-System seien aufgrund einer Störung oder Softwareaktualisierung die Benutzerdaten verloren gegangen und der Kunde solle die Daten auf der Bankseite bestätigen oder ändern. Folgt der Benutzer dem Link, der auf die Webseite der Angreifer führt, und gibt dort seine Daten ein, so fallen diese den Angreifern in die Hände.

Für den Schutz vor Phishing ist Anti-Phishing verantwortlich, das zu den Komponenten Web-Anti-Virus, Anti-Spam und IM-Anti-Virus gehört. Aktivieren Sie diese Komponenten, um einen effektiven Schutz vor Phishing zu gewährleisten.

Gehen Sie folgendermaßen vor, um die Komponenten für den Phishing-Schutz zu aktivieren:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Schutz-Center**.

2. Öffnen Sie auf der rechten Fensterseite durch Linksklick den Block **Kontrolle der Arbeit im Netzwerk**.

3. Klicken Sie auf **Anti-Phishing**, um das Menü zur Auswahl einer Aktion für die Komponente zu öffnen, und wählen Sie im Menü den Punkt **Anti-Phishing aktivieren**.

   Anti-Phishing und die Komponenten, zu denen Anti-Phishing gehört, werden aktiviert.

VIRTUELLE TASTATUR

Bei der Arbeit auf einem Computer ist es häufig erforderlich, persönliche Daten, Benutzername und Kennwort einzugeben. Beispiele sind die Anmeldung auf Webseiten, der Besuch von Online-Shops und die Verwendung von Online-Banking.

In solchen Situationen besteht die Gefahr, dass persönliche Informationen mit Hilfe von Hardware-Hooks oder mit Keyloggern (Programme, die Tasteneingaben registrieren) abgefangen werden.

Die Virtuelle Tastatur ermöglicht es, das Abfangen von über die Tastatur eingegebenen Daten zu verhindern.

Die Virtuelle Tastatur kann Ihre persönlichen Daten nicht schützen, wenn eine Webseite gehackt wurde und die Eingabe solcher Daten fordert, weil die Informationen in diesem Fall dem Angreifer direkt in die Hände fallen.

Viele Spyware-Programme besitzen Funktionen zum Anlegen von Screenshots, die an Angreifer für Analyse und Sammeln von persönlichen Benutzerdaten automatisch übergeben werden. Die Virtuelle Tastatur schützt vor Abfangen von eingegebenen persönlichen Daten durch Anlegen von Screenshots.

Die Virtuelle Tastatur schützt persönliche Daten nur dann vor Diebstahlversuchen, wenn Sie mit den Internetbrowsern Microsoft Internet Explorer und Mozilla Firefox arbeiten.

Beachten Sie die Besonderheiten für die Verwendung der Virtuellen Tastatur, bevor Sie diese einsetzen:

- Überzeugen Sie sich vor der Dateneingabe mittels virtueller Tastatur davon, dass sich der Mauscursor im entsprechenden Eingabefeld befindet.

- Die Betätigung der Tasten der virtuellen Tastatur erfolgt durch Mausklick.

- Im Gegensatz zu einer echten Tastatur ist es auf der Virtuellen Tastatur nicht möglich, gleichzeitig zwei Tasten zu drücken. Um Tastenkombinationen zu verwenden (z.B. **ALT+F4**), ist es deshalb notwendig, zuerst die erste Taste (z.B. **ALT**), dann die zweite Taste (z.B. **F4**) und anschließend erneut die erste Taste zu drücken. Das wiederholte Drücken ersetzt das Loslassen einer Taste auf der echten Tastatur.

- Auf der Virtuellen Tastatur wird die Eingabesprache mit dem Tastenkürzel **STRG+UMSCHALT** geändert (wobei mit der rechten Maustaste auf die Taste **Umschalt** gedrückt wird) oder mit **STRG+NACH LINKS ALT** (wobei mit der rechten Maustaste auf **NACH LINKS ALT** gedrückt wird). Die Kombination ist von den festgelegten Einstellungen abhängig.

Das Öffnen der virtuellen Tastatur kann auf mehrere Arten erfolgen:

- Aus dem Kontextmenü des Programms.

- aus dem

- aus den Fenstern der Browser Microsoft Internet Explorer oder Mozilla Firefox.

- mit Hilfe einer Tastenkombination.

- *Um die Virtuelle Tastatur vom Kontextmenü aus zu öffnen,*

  wählen Sie im Kontextmenü des Programmsymbols den Punkt **Tools** → **Virtuelle Tastatur**.

- *Um die virtuelle Tastatur aus dem Hauptfenster des Programms zu öffnen,*

  klicken Sie unter **Sichere Umgebung** im Programmhauptfenster auf **Virtuelle Tastatur**.

- *Um die virtuelle Tastatur von einem Browserfenster aus zu öffnen,*

  klicken Sie auf die Schaltfläche **Virtuelle Tastatur** in der Symbolleiste von Microsoft Internet Explorer oder Mozilla Firefox.

- *Um die virtuelle Tastatur mit Hilfe der Computertastatur zu öffnen,*

  betätigen Sie die Tastenkombination **STRG+ALT+UMSCHALT+P**.

WAS TUN, WENN SIE VERMUTEN, DASS EIN OBJEKT VON EINEM VIRUS INFIZIERT IST?

Wenn Sie den Verdacht haben, dass ein Objekt infiziert ist, sollten Sie es zuerst mit Hilfe von Kaspersky Internet Security untersuchen (s. Abschnitt "Untersuchung von Dateien, Ordnern, Laufwerken und anderen Objekten auf Viren" auf S. 64).

Wenn ein Objekt bei der Untersuchung vom Programm als virenfrei eingestuft wird, Sie aber vermuten, dass es infiziert ist, können Sie folgendermaßen vorgehen:

- Objekt in die *Quarantäne* verschieben. Objekte, die in die Quarantäne verschoben wurden, stellen keine Gefahr für Ihren Computer dar. Möglicherweise kann die Bedrohung eindeutig bestimmt und desinfiziert werden, nachdem die Datenbanken von Kaspersky Internet Security aktualisiert wurden.

- Objekt an das *Virenlabor* schicken. Die Experten des Virenlabors untersuchen das Objekt. Falls es tatsächlich infiziert ist, wird den Datenbanken eine Beschreibung des neuen Virus hinzugefügt. Die Datenbanken werden beim Update vom Programm aktualisiert (s. Abschnitt "Aktualisierung von Programmdatenbanken und -modulen" auf S. 62).

Ein Objekt kann auf zwei Arten in die Quarantäne verschoben werden:

- mit dem Link **In die Quarantäne verschieben** im Fenster **Schutzstatus**.

- mit Hilfe des Kontextmenüs für ein Objekt

- *Gehen Sie folgendermaßen vor, um vom Fenster Schutzstatus aus ein Objekt in die Quarantäne zu verschieben:*

  1. Öffnen Sie das Programmhauptfenster.

  2. Klicken Sie im Hauptfenster oben auf den Link **Quarantäne**, um das Fenster **Schutzstatus** auf der Registerkarte **Erkannte Bedrohungen** zu öffnen.

  3. Klicken Sie auf **In Quarantäne verschieben**.

  4. Wählen Sie im folgenden Fenster das Objekt, das in die Quarantäne verschoben werden soll.

- *Gehen Sie folgendermaßen vor, um ein Objekt mit Hilfe des Kontextmenüs in die Quarantäne zu verschieben:*

  1. Öffnen Sie das Fenster von Microsoft Windows Explorer und gehen Sie in den Ordner mit dem Objekt, das in die Quarantäne verschoben werden soll.

2. Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt und wählen Sie den Punkt **In die Quarantäne verschieben**.

Gehen Sie folgendermaßen vor, um ein Objekt an das Virenlabor zu schicken:

1. Gehen Sie auf die Seite, die zum Senden einer Anfrage an das Virenlabor (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de) dient.

2. Folgen Sie den Anweisungen, die auf dieser Seite gegeben werden, um eine Anfrage zu schicken.

WIE MIT EINER GROßEN ANZAHL VON SPAM-MAILS VERFAHREN WIRD?

Wenn Sie viel Spam erhalten, aktivieren Sie die Komponente Anti-Spam, wählen Sie die empfohlene Sicherheitsstufe und trainieren Sie die Komponente dann mit dem *Trainingsassistenten*. Für die korrekte Spam-Erkennung ist es erforderlich, ein Training mit mindestens 50 Mustern erwünschter Mails und 50 Spam-Mustern vorzunehmen.

Gehen Sie folgendermaßen vor, um Anti-Spam zu aktivieren und die empfohlene Sicherheitsstufe zu wählen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Anti-Spam aktivieren**.

4. Im Block **Sicherheitsstufe** ist standardmäßig die Sicherheitsstufe **Empfohlen** eingestellt.

   Sollte die Sicherheitsstufe **Niedrig** oder **Benutzerdefiniert** gewählt sein, so klicken Sie auf **Standard**. Die Sicherheitsstufe erhält automatisch den Wert **Empfohlen**.

Gehen Sie folgendermaßen vor, um Anti-Spam mit Hilfe des Trainingsassistenten zu trainieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Klicken Sie auf der rechten Fensterseite im Block **Anti-Spam-Training** auf **Trainieren**.

   Das Fenster des Trainingsassistenten wird geöffnet.

Details zu den einzelnen Schritte des Assistenten

Schritt 1. Assistent starten

Klicken Sie auf **Weiter**, um mit dem Training zu beginnen.

Schritt 2. Ordner wählen, die erwünschte E-Mails enthalten

Auf dieser Etappe können Sie die Ordner wählen, die erwünschte E-Mails enthalten. Es dürfen nur Ordner gewählt werden, über deren Inhalt vollständige Sicherheit besteht.

> Nur die Ordner von Benutzerkonten für Microsoft Office Outlook und Microsoft Outlook Express (Windows Mail) stehen zur Auswahl.

Schritt 3. Ordner wählen, die unerwünschte E-Mails enthalten

Auf dieser Etappe können Sie die Ordner wählen, die unerwünschte E-Mails (Spam) enthalten. Sollten in Ihrem Mailprogramm keine entsprechenden Ordner vorhanden sein, dann überspringen Sie diesen Schritt.

Nur die Ordner von Benutzerkonten für Microsoft Office Outlook und Microsoft Outlook Express (Windows Mail) stehen zur Auswahl.

Schritt 4. Anti-Spam-Training

Bei diesem Schritt findet das automatische Training von Anti-Spam statt. Dazu dienen die Ordner, die bei den vorhergehenden Schritten ausgewählt wurden. Die Anti-Spam-Datenbank wird durch die E-Mails aus diesen Ordnern ergänzt. Die Absender von erwünschten E-Mails werden automatisch in die Liste der erlaubten Absender aufgenommen.

Schritt 5. Trainingsergebnisse speichern

Auf dieser Etappe des Assistenten werden die Trainingsergebnisse auf eine der folgenden Arten gespeichert:

- Trainingsergebnisse zur bestehenden Anti-Spam-Datenbank hinzufügen (Variante **Anti-Spam-Datenbank durch Trainingsergebnisse ergänzen**).
- Bestehende Datenbank durch die neu erstellte Datenbank ersetzen (Variante **Neue Anti-Spam-Datenbank erstellen**).

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

WAS TUN, WENN SIE VERMUTEN, DASS IHR COMPUTER INFIZIERT IST?

Wenn Sie vermuten, dass Ihr Computer infiziert ist, verwenden Sie den *Assistenten zur Systemwiederherstellung*, der die Spuren von schädlichen Objekten im System beseitigt. Die Kaspersky-Lab-Experten empfehlen außerdem, den Assistenten nach einer Desinfektion des Computers auszuführen, um sicherzustellen, dass alle aufgetretenen Bedrohungen und Beschädigungen beseitigt wurden.

Der Assistent prüft, ob im System Veränderungen vorliegen. Dazu zählen z.B. blockierter Zugriff auf die Netzwerkumgebung, veränderte Dateierweiterungen bekannter Formate, blockierte Systemsteuerung usw. Es gibt unterschiedliche Gründe für das Auftreten solcher Beschädigungen. Es kann sich um die Aktivität schädlicher Programme, inkorrekte Systemeinstellungen, Systemabstürze oder die Verwendung inkorrekt funktionierender Systemoptimierungsprogramme handeln.

Nach der Untersuchung analysiert der Assistent die gesammelten Informationen, um festzustellen, ob im System Beschädigungen vorliegen, die sofort behoben werden müssen. Aufgrund der Untersuchungsergebnisse wird eine Liste von Aktionen erstellt, die ausgeführt werden müssen, um die Beschädigungen zu beheben. Der Assistent ordnet die Aktionen nach der Priorität der gefundenen Probleme in Kategorien an.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Gehen Sie folgendermaßen vor, den Assistenten zur Systemwiederherstellung zu starten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Tools**.
2. Klicken Sie auf der rechten Fensterseite auf Wiederherstellung nach Infektion.

Details zu den einzelnen Schritte des Assistenten

Schritt 1. Systemwiederherstellung starten

Vergewissern Sie sich, dass im Assistentenfenster die Variante **Suche nach Problemen, die mit Malware-Aktivität zusammenhängen, durchführen** gewählt wurde, und klicken Sie auf **Weiter**.

Schritt 2. Nach Problemen suchen

Der Assistent sucht nach Problemen und möglichen Beschädigungen, die behoben werden müssen. Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 3. Aktionen für die Problembehebung wählen

Alle Beschädigungen, die beim vorherigen Schritt gefunden wurden, werden ihrer Gefährlichkeit nach angeordnet. Für jede Gruppe von Beschädigungen schlagen die Kaspersky-Lab-Spezialisten eine Auswahl von Aktionen vor, deren Ausführung die Beschädigungen beheben kann. Die Aktionen sind in drei Gruppen unterteilt:

- *Ausdrücklich empfohlene Aktionen* können Beschädigungen beheben, die ein ernsthaftes Problem darstellen. Es wird empfohlen, alle Aktionen dieser Gruppe auszuführen.
- *Empfohlene Aktionen* dienen zum Beheben von Beschädigungen, die ein potentielles Risiko darstellen können. Es wird empfohlen, auch alle Aktionen dieser Gruppe auszuführen.
- *Zusätzliche Aktionen* dienen dazu, momentan ungefährliche Beschädigungen des Systems zu beheben, die die Computersicherheit in Zukunft bedrohen können.

Klicken Sie links vom Namen einer Gruppe auf das Zeichen **+**, um die Aktionen der Gruppe anzuzeigen.

Um eine bestimmte Aktion auszuführen, aktivieren Sie das Kontrollkästchen links vom Namen der Aktion. In der Grundeinstellung werden alle empfohlenen und ausdrücklich empfohlenen Aktionen ausgeführt. Soll eine bestimmte Aktion nicht ausgeführt werden, dann deaktivieren Sie das entsprechende Kontrollkästchen

Die standardmäßig aktivierten Kontrollkästchen sollten auf keinen Fall entfernt werden, weil dadurch die Sicherheit Ihres Computers bedroht wird.

Klicken Sie auf **Weiter**, nachdem Sie die Aktionen gewählt haben, die der Assistent ausführen soll.

Schritt 4. Probleme beheben

Der Assistent führt die Aktionen aus, die beim vorherigen Schritt festgelegt wurden. Die Problembehebung kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Problembehebung automatisch zum nächsten Schritt.

Schritt 5. Assistent abschließen

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

WIE EIN OBJEKT WIEDERHERGESTELLT WIRD, DAS VOM PROGRAMM GELÖSCHT ODER DESINFIZIERT WURDE.

Kaspersky Lab warnt davor, gelöschte und desinfizierte Objekte wiederherzustellen, weil diese eine Gefahr für Ihren Computer darstellen können.

Wenn die Wiederherstellung eines gelöschten oder desinfizierten Objekts erforderlich ist, verwenden Sie dazu die Sicherungskopie, die vom Programm bei der Untersuchung des Objekts angelegt wurde.

Gehen Sie folgendermaßen vor, um ein Objekt wiederherzustellen, das vom Programm gelöscht oder desinfiziert wurde:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im Hauptfenster oben auf den Link **Quarantäne**, um das Fenster **Schutzstatus** auf der Registerkarte **Erkannte Bedrohungen** zu öffnen.

3. Wählen Sie in der Dropdown-Liste oberhalb der Liste der Bedrohungen das Element **Neutralisierte** aus.

   Die Registerkarte **Erkannte Bedrohungen** enthält eine Liste der desinfizierten und gelöschten Objekte. Die Objekte sind ihrem Status nach angeordnet. Klicken Sie links von der Überschrift einer Gruppe auf das Zeichen **+**, um eine Liste mit den Objekten einer Gruppe anzuzeigen.

4. Öffnen Sie durch Rechtsklick das Kontextmenü für das wiederherzustellende Objekt und wählen Sie im Menü den Punkt **Wiederherstellen**.

WIE EINE NOTFALL-CD ERSTELLT UND VERWENDET WIRD.

Es wird empfohlen, Kaspersky Internet Security auf dem Computer zu installieren und anzupassen, und den Computer dann zu untersuchen, um sicherzustellen, dass er virenfrei ist. Anschließend können Sie eine Notfall-CD erstellen. Die Notfall-CD kann später verwendet werden, um den infizierten Computer zu untersuchen und zu desinfizieren, wenn eine Desinfektion mit anderen Mitteln (z.B. Antiviren-Programme) fehlschlägt.

IN DIESEM ABSCHNITT

Notfall-CD erstellen 73

Hochfahren eines Computers mit Hilfe der Notfall-CD 75

NOTFALL-CD ERSTELLEN

Das Anlegen einer Notfall-CD umfasst das Erstellen eines Disk-Abbild (iso-Datei) mit den aktuellen Programm-Datenbanken und Konfigurationsdateien.

Ein Original des Disk-Abbilds, auf dessen Basis eine neue Datei erstellt wird, kann von einem Kaspersky-Lab-Server heruntergeladen oder aus einer lokalen Quelle kopiert werden.

Die Notfall-CD wird mit Hilfe des *Assistenten zum Erstellen einer Notfall-CD* erstellt. Die vom Assistenten angelegte Abbild-Datei rescuecd.iso wird auf der Festplatte Ihres Computers gespeichert:

- im Betriebssystem Microsoft Windows XP – im Ordner Dokumente und Einstellungen\All Users\Application Data\Kaspersky Lab\AVP11\Data\Rdisk\.

- in Betriebssystemen Microsoft Windows Vista und Microsoft Windows 7 – im Ordner ProgramData\Kaspersky Lab\AVP11\Data\Rdisk\.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Gehen Sie folgendermaßen vor, um Assistenten zum Erstellen einer Notfall-CD zu starten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Tools**.

2. Klicken Sie auf der rechten Fensterseite auf

3. **Notfall-CD**.

Details zu den einzelnen Schritte des Assistenten

Schritt 1. Assistent starten. Suche nach einem existierenden Festplattenabbild

Im ersten Fenster des Assistenten werden Informationen über die Notfall-CD angezeigt, die durch den Assistenten erstellt wird.

Erkennt der Assistent in dem dafür vorgesehenen Ordner (s. oben) ein bereits vorhandenes Abbild der Notfall-CD, so wird im ersten Fenster des Assistenten das Kontrollkästchen **Vorhandenes Abbild verwenden** angezeigt. Aktivieren Sie das Kontrollkästchen, um die erkannte Datei als Basis für das Disk-Abbild zu verwenden und direkt zum Schritt **Abbild aktualisieren** zu wechseln (s. unten). Deaktivieren Sie dieses Kontrollkästchen, wenn Sie das gefundene Festplattenabbild nicht verwenden wollen – der Assistent wechselt dann zum Fenster **Quelle für Disk-Abbild wählen**.

Schritt 2. Quelle für Disk-Abbild wählen

Wenn Sie im ersten Fenster des Assistenten das Kontrollkästchen **Vorhandenes Abbild verwenden**, aktiviert haben, wird dieser Schritt übersprungen.

Auf dieser Etappe muss aus folgenden Varianten eine Quelle für die Abbild-Datei gewählt werden:

- Wählen Sie die Variante **Abbild von lokaler Festplatte oder Netzlaufwerk kopieren**, wenn Sie über eine fertige Notfall-CD verfügen oder auf Ihrem Computer bzw. in einer Ressource des lokalen Netzwerks ein dafür vorbereitetes Abbild bereitliegt.

- Wählen Sie die Variante **Abbild von Kaspersky-Lab-Server herunterladen**, wenn Sie nicht über eine fertige Abbild-Datei verfügen und diese von einem Kaspersky-Lab-Server herunterladen möchten (die Dateigröße beträgt ungefähr 175 MB).

Schritt 3. Disk-Abbild kopieren (herunterladen)

Wenn Sie im ersten Fenster des Assistenten das Kontrollkästchen **Vorhandenes Abbild verwenden**, aktiviert haben, wird dieser Schritt übersprungen.

Wenn Sie beim vorherigen Schritt die Variante zum Kopieren des Abbild aus einer lokalen Quelle gewählt haben (**Abbild von lokaler Festplatte oder Netzlaufwerk kopieren**), geben Sie bei diesem Schritt den entsprechenden Pfad an. Klicken Sie dazu auf die Schaltfläche **Durchsuchen**. Nachdem Sie den Pfad zur Datei angegeben haben, klicken Sie auf **Weiter**. Im Assistentenfenster wird angezeigt, wie das Kopieren des Disk-Abbilds verläuft.

Wenn Sie die Variante **Abbild von Kaspersky-Lab-Server herunterladen**, gewählt haben, wird sofort angezeigt, wie das Kopieren des Disk-Abbilds verläuft.

Nach Abschluss des Kopiervorgangs oder des Ladens des Disk-Abbilds wechselt der Assistent automatisch zum nächsten Schritt.

Schritt 4. Abbild-Datei aktualisieren

Der Vorgang zur Aktualisierung der Abbild-Datei umfasst:

- Update der Antiviren-Datenbanken.

- Aktualisierung der Konfigurationsdateien.

Die Konfigurationsdateien bestimmen die Möglichkeit zum Hochfahren des Computers von einem Wechseldatenträger oder einer CD / DVD, auf denen ein Abbild der Notfall-CD gespeichert wurde, das wiederum unter Verwendung des Assistenten erstellt wurde.

Für die Aktualisierung der Antiviren-Datenbanken werden die beim letzten Update von Kaspersky Internet Security heruntergeladenen Datenbanken verwendet. Wenn die Datenbanken veraltet sind, wird empfohlen, die Updateaufgabe auszuführen und den Notfall-CD-Assistenten erneut zu starten.

Klicken Sie auf **Weiter**, um die Aktualisierung der Datei zu starten. Im Assistentenfenster wird angezeigt, wie die Aktualisierung verläuft.

Schritt 5. Schreiben eines Abbilds auf Datenträger

In diesem Fenster informiert der Assistent Sie darüber, dass die Notfall-CD erfolgreich erstellt wurde, und schlägt Ihnen vor, ein Abbild auf einen Datenträger zu schreiben.

Geben Sie den Datenträger an, auf den das Disk-Abbild geschrieben werden soll:

- Wählen Sie die Option **Auf CD/DVD schreiben** aus, um das Abbild auf CD/DVD zu schreiben.

  Ihnen wird vorgeschlagen, die CD/DVD anzugeben, auf die das Abbild geschrieben werden soll, woraufhin das Schreiben des Abbilds auf dieser CD/DVD erfolgt. Der Schreibvorgang kann eine gewisse Zeit beanspruchen - warten Sie, bis dieser abgeschlossen ist.

- Wählen Sie die Option **Auf USB-Gerät schreiben** aus, um das Abbild auf einen Wechseldatenträger zu schreiben.

  Kaspersky Lab rät davon ab, Disk-Abbilder auf Geräten zu speichern, die nicht ausschließlich für die Datenspeicherung konzipiert sind, wie z.B. Smartphones, Mobiltelefone, PDAs und MP3-Player. Solche Geräte können bei Verwendung für die Speicherung von Disk-Abbildern in ihrer Funktion beeinträchtigt werden.

  Ihnen wird vorgeschlagen, den Wechseldatenträger anzugeben, auf den das Abbild geschrieben werden soll, woraufhin das Schreiben des Abbilds auf diesem Wechseldatenträger erfolgt. Der Schreibvorgang kann eine gewisse Zeit beanspruchen - warten Sie, bis dieser abgeschlossen ist.

- Wählen Sie die Option **Abbild in einer Datei auf lokaler Festplatte oder Netzlaufwerk speichern**, um das Disk-Abbild auf der Festplatte Ihres Computers oder auf einem anderen Computer zu speichern, auf den Sie über das Netzwerk Zugriff haben.

  Ihnen wird vorgeschlagen, einen Ordner anzugeben, in dem das Abbild gespeichert werden soll, sowie auch den Namen der Abbild-Datei, woraufhin das Speichern des Abbilds auf der Festplatte erfolgt. Der Schreibvorgang kann eine gewisse Zeit beanspruchen - warten Sie, bis dieser abgeschlossen ist.

Schritt 6. Assistent abschließen

Klicken Sie auf **Beenden**, um die Arbeit des Assistenten abzuschließen Die erstellte Disk können Sie für das nachfolgende Booten des Computers verwenden (s. S. 75).

HOCHFAHREN EINES COMPUTERS MIT HILFE DER NOTFALL-CD

Wenn sich das Betriebssystem aufgrund eines Virenangriffs nicht mehr hochfahren lässt, können Sie die Notfall-CD einsetzen.

Um das Betriebssystem zu booten, ist eine CD/DVD oder ein Wechseldatenträger mit der darauf gespeicherten Abbild-Datei (.iso) der Boot-Disk erforderlich (s. Abschnitt "Notfall-CD erstellen" auf S. 73).

Ein Booten des Computers von einem Wechseldatenträger ist nicht immer möglich. Dies wird beispielsweise von einigen älteren Computermodellen nicht unterstützt. Klären Sie vor dem Herunterfahren des Computers für ein nachfolgendes Booten vom Wechseldatenträger, ob diese Möglichkeit gegeben ist.

Gehen Sie folgendermaßen vor, um den Computer von einer Notfall-CD zu booten:

1. Wählen Sie in den BIOS-Einstellungen das Booten von CD / DVD oder Wechseldatenträger (weitere Informationen können der Dokumentation zum Motherboard Ihres Computers entnommen werden).

2. Legen Sie die CD/DVD mit dem vorher darauf gespeicherten Disk-Abbild in das CD/DVD-Laufwerk des infizierten Computers ein oder schließen Sie den entsprechend vorbereiteten Wechseldatenträger an.

3. Starten Sie den Computer neu.

Ausführliche Informationen über die Verwendung der Notfall-CD bietet das Benutzerhandbuch zu Kaspersky Rescue Disk.

AUFRUFEN DES BERICHTS ÜBER DIE PROGRAMMAKTIVITÄT

Kaspersky Internet Security führt Berichte über die Arbeit aller Komponenten. Im Bericht können Sie beispielsweise feststellen, wie viele schädliche Objekte (z.B. Viren, trojanische Programme) das Programm in einem bestimmten Zeitraum gefunden und neutralisiert hat, wie oft das Programm in diesem Zeitraum aktualisiert wurde, wie viele Spam-Mails gefunden wurden, u.a.

Bei der Arbeit auf einem Computer mit dem Betriebssystem Microsoft Windows Vista oder Microsoft Windows 7 können Sie mit Hilfe des Kaspersky Gadgets die Berichte öffnen. Dafür muss eine der Schaltflächen des Kaspersky Gadgets mit der Funktion zum Anhalten des Schutzes belegt sein (s. Abschnitt "Wie wird das Kaspersky Gadget verwendet?" auf S. 78).

Gehen Sie folgendermaßen vor, um einen Bericht über die Programmarbeit anzuzeigen:

1. Verwenden Sie eine der folgenden Methoden, um das Fenster **Schutzstatus** auf der Registerkarte **Bericht** zu öffnen:

   - verwenden Sie im oberen Bereich des Programmhauptfensters den Link **Berichte**.

   - klicken Sie im Interface des Kaspersky Gadgets auf die Schaltfläche mit dem Symbol **Berichte** (nur für die Betriebssysteme Microsoft Windows Vista und Microsoft Windows 7).

   Auf der Registerkarte **Bericht** werden die Programmberichte in Form von Diagrammen dargestellt.

2. Klicken Sie im unteren Bereich der Registerkarte **Bericht** auf **Detallierter Bericht**, um einen ausführlichen Bericht über die Arbeit des Programms zu öffnen (z.B. über die Arbeit der einzelnen Programmkomponenten).

   Das Fenster **Detallierter Bericht** wird geöffnet. Hier werden die Daten in Tabellenform dargestellt. Die Berichtseinträge können auf unterschiedliche Weise angeordnet werden.

WIE WERDEN DIE STANDARDEINSTELLUNGEN DES PROGRAMMS WIEDERHERGESTELLT?

Sie können jederzeit zu den Einstellungen für Kaspersky Internet Security zurückkehren, die von Kaspersky Lab empfohlen werden udn als optimal gelten. Die Wiederherstellung der Einstellungen erfolgt mit Hilfe des *Konfigurationsassistenten für das Programm*.

Der Assistent stellt für alle Schutzkomponenten die Sicherheitsstufe **Empfohlen** ein. Bei der Wiederherstellung der Einstellungen können Sie außerdem festlegen, welche Parameter bei der Wiederherstellung der empfohlenen Sicherheitsstufe beibehalten werden sollen und für welche Komponenten diese Parameter gelten sollen.

Gehen Sie folgendermaßen vor, um die Schutzeinstellungen wiederherzustellen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Starten Sie den Konfigurationsassistenten für das Programm mit einer der folgenden Methoden:

   - Klicken Sie im unteren Fensterbereich auf den Link **Wiederherstellen**.

   - Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Unterabschnitt **Programmkonfiguration** und klicken Sie im Block **Standardeinstellungen wiederherstellen** auf **Wiederherstellen**.

Details zu den einzelnen Schritte des Assistenten

Schritt 1. Assistent starten

Klicken Sie auf den Link **Weiter**, um den Assistenten fortzusetzen.

Schritt 2. Zu speichernde Parameter wählen

Das Fenster enthält die Komponenten von Kaspersky Internet Security, deren Parameter vom Benutzer verändert oder von Kaspersky Internet Security beim Training der Komponenten Firewall und Anti-Spam gesammelt wurden. Wenn für eine bestimmte Komponente bei der Arbeit unikale Parameter festgelegt wurden, werden diese ebenfalls im Fenster angegeben.

Als unikale Parameter gelten: Erlaubnisliste und Verbotsliste mit Phrasen und Adressen für die Komponente Anti-Spam, Listen mit vertrauenswürdigen Internetadressen und Telefonnummern von Internetprovidern, die von den Komponenten Web-Anti-Virus und Anti-Spy verwendet werden, für den Schutz geltende Ausnahmeregeln, Firewall-Filterregeln für Pakete und Programme.

Diese Listen werden während der Arbeit von Kaspersky Internet Security erstellt. Dabei werden individuelle Aufgaben und Sicherheitsanforderungen berücksichtigt. Das Erstellen der Listen ist sehr zeitaufwändig. Deshalb wird empfohlen, sie beim Wiederherstellen der ursprünglichen Programmeinstellungen zu speichern.

Aktivieren Sie die Kontrollkästchen für die Parameter, die gespeichert werden sollen, und klicken Sie dann auf **Weiter**.

Schritt 3. Systemanalyse

Auf dieser Etappe werden Informationen über Programme, die zu Microsoft Windows gehören, gesammelt. Diese Programme werden in die Liste der vertrauenswürdigen Anwendungen aufgenommen, deren Aktionen im System nicht beschränkt werden.

Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 4. Wiederherstellung abschließen

Klicken Sie auf **Beenden**, um die Arbeit des Assistenten abzuschließen

WIE PROGRAMMEINSTELLUNGEN VON KASPERSKY INTERNET SECURITY AUF EINEN ANDEREN COMPUTER ÜBERTRAGEN WERDEN.

Sie können Ihre Programmeinstellungen für ein anderes Exemplar von Kaspersky Internet Security übernehmen, das auf einem anderen Computer installiert ist. Auf diese Weise sind die Einstellungen des Programms auf beiden Computern identisch. Diese Option kann beispielsweise von Nutzen sein, wenn Sie Kaspersky Internet Security auf einem PC zuhause und im Büro installiert haben.

Die Programmeinstellungen werden in einer speziellen Konfigurationsdatei gespeichert, die Sie von Computer zu Computer übertragen können. Dabei gilt folgendes Vorgehen:

1. *Exportieren* Sie die Einstellungen, d.h. die Programmeinstellungen werden in eine Konfigurationsdatei kopiert.
2. Übertragen Sie die gespeicherte Datei auf einen anderen Computer (z.B. per E-Mail oder mit einem Wechseldatenträger).
3. *Importieren* Sie die Einstellungen, d.h. die Einstellungen werden aus einer Konfigurationsdatei in ein Programm übernommen, das auf einem anderen Computer installiert ist.

Gehen Sie folgendermaßen vor, um die aktuellen Funktionsparameter von Kaspersky Internet Security zu exportieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Programmkonfiguration**.
3. Klicken Sie auf der rechten Fensterseite auf **Speichern**.
4. Geben Sie im folgenden Fenster einen Namen für die Konfigurationsdatei an und wählen Sie einen Speicherort dafür aus.

Gehen Sie folgendermaßen vor, um die Funktionsparameter aus einer Konfigurationsdatei zu importieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Programmkonfiguration**.
3. Klicken Sie auf der rechten Fensterseite auf **Laden**.
4. Wählen Sie im folgenden Fenster eine Datei aus, aus der Sie die Parameter für Kaspersky Internet Security importieren möchten.

WIE DAS KASPERSKY GADGET VERWENDET WIRD.

Wenn Kaspersky Internet Security auf einem Computer mit dem Betriebssystem Microsoft Windows Vista oder Microsoft Windows 7 eingesetzt wird, steht das Kaspersky Gadget zur Verfügung (weiter auch einfach als *Gadget* bezeichnet).

Nach der Installation von Kaspersky Internet Security auf einem Computer mit dem Betriebssystem Microsoft Windows 7 erscheint das Gadget automatisch auf dem Desktop. Wenn das Programm auf einem Computer mit dem Betriebssystem Microsoft Windows Vista installiert wird, muss das Gadget manuell zur Sidebar von Microsoft Windows hinzugefügt werden (s. Dokumentation des Betriebssystems).

Der Farbindikator des Gadgets signalisiert den Schutzstatus Ihres Computers. Er entspricht dem Indikator für den Schutzstatus im Programmhauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47). Die Farbe Grün bedeutet, dass der Computer sicher ist. Gelb signalisiert, dass der Schutz Probleme aufweist, und Rot warnt vor einer ernsthaften Bedrohung für die Computersicherheit. Ist der Indikator grau, so wurde das Programm angehalten.

Das Aussehen des Gadgets informiert auch über den Update-Download: Während einer Aktualisierung der Datenbanken und Programm-Module erscheint in der Mitte des Gadgets ein rotierender Globus.

Mit Hilfe des Gadgets können Sie folgende wichtige Aufgaben ausführen:

- Programm starten, wenn es angehalten wurde.
- Programmhauptfenster öffnen
- einzelne Objekte auf Viren untersuchen
- News-Fenster öffnen

Um das Programm mit Hilfe des Gadgets zu starten,

klicken Sie in der Mitte des Gadgets auf das Symbol **Aktivieren**.

Um das Programmhauptfenster mit Hilfe des Gadgets zu öffnen:

klicken Sie in der Mitte des Gadgets auf das Symbol von Kaspersky Internet Security.

Um ein Objekt mit Hilfe des Gadgets auf Viren zu untersuchen,

ziehen Sie das Untersuchungsobjekt auf das Gadget.

Der Vorgang der Aufgabenausführung wird im folgenden Fenster **Auf Viren untersuchen** angezeigt.

Um mit Hilfe des Gadgets das Fenster zur Anzeige der Neuigkeiten zu öffnen:

klicken Sie auf das Symbol , das beim Erscheinen von Neuigkeiten in der Mitte des Gadgets erscheint.

Gadget anpassen

Sie können das Gadget so anpassen, dass mit den Schaltflächen folgende Aktionen ausgeführt werden können:

- Programmparameter ändern.
- Programmberichte anzeigen.
- zum sicheren Desktop umschalten (nur für 32-Bit-Betriebssysteme)
- Berichte über Kindersicherung anzeigen.
- Informationen zur Netzwerk-Aktivität anzeigen (Netzwerkmonitor).
- Schutz anhalten.

Außerdem können Sie das Aussehen des Gadgets ändern, indem Sie eine grafische Oberfläche für das Gadget auswählen.

Gehen Sie folgendermaßen vor, um das Gadget anzupassen:

1. Öffnen Sie das Gadget-Konfigurationsfenster durch Klick auf das Symbol , das rechts oben im Gadget-Block erscheint, wenn mit der Maus darauf gezeigt wird.
2. Wählen Sie aus den Dropdown-Listen **Linkes Symbol** und **Rechtes Symbol** die Aktionen, die bei Klick auf die linke und rechte Gadget-Schaltfläche ausgeführt werden sollen.
3. Wählen Sie durch Klick auf die Schaltfläche eine grafische Oberfläche für das Gadget.

4. Klicken Sie auf **OK**, um die vorgenommenen Änderungen zu speichern.

ERWEITERTE PROGRAMMEINSTELLUNGEN

Dieser Abschnitt informiert ausführlich über die einzelnen Komponenten und beschreibt den jeweiligen Funktionsalgorithmus und die Einstellungen.

Verwenden Sie eine der folgenden Methoden, um zu den erweiterten Einstellungen für das Programm zu gelangen:

- verwenden Sie im oberen Bereich des Programmhauptfensters den Link **Einstellungen**.
- wählen Sie im Kontextmenü des Programmsymbols den Punkt **Einstellungen**.

IN DIESEM ABSCHNITT

Grundlegende Schutzparameter 82

Untersuchung des Computers 84

Update 92

Datei-Anti-Virus 97

Mail-Anti-Virus 103

Web-Anti-Virus 108

IM-Anti-Virus 117

Proaktiver Schutz 119

Aktivitätsmonitor 121

Programmkontrolle 123

Netzwerkschutz 132

Anti-Spam 143

Anti-Banner 160

Sichere Umgebung 163

Kindersicherung 169

Vertrauenswürdige Zone 179

Leistung und Kompatibilität mit anderen Programmen 181

Selbstschutz für Kaspersky Internet Security 185

Quarantäne und Backup 186

Zusätzliche Schutz-Tools 188

Berichte 193

Aussehen des Programms 197

Meldungen 199

Teilnahme an Kaspersky Security Network 201

GRUNDLEGENDE SCHUTZPARAMETER

Im Fenster mit den Programmeinstellungen können Sie unter **Allgemeine Einstellungen** im Abschnitt **Schutz-Center** die folgenden Operation ausführen:

- alle Schutzkomponenten deaktivieren (s. Abschnitt "Schutz aktivieren und deaktivieren" auf S. 57);
- automatischen oder interaktiven Schutzmodus auswählen (s. Abschnitt"Schutzmodus auswählen" auf S. 83);

- Zugriff der Benutzer auf das Programm mittels Kennwort beschränken (s. Abschnitt "Kontrolle des Zugriffs auf Kaspersky Internet Security" auf S. 83);
- utomatischen Programmstart bei Hochfahren des Betriebssystems aktivieren oder deaktivieren (s. Abschnitt "Automatischen Start aktivieren und deaktivieren" auf S. 54);
- festgelegte Tastenkombination zur Anzeige der virtuellen Tastatur auf dem Bildschirm aktivieren (s. Abschnitt "Virtuelle Tastatur" auf S. 68).

IN DIESEM ABSCHNITT

Kontrolle des Zugriffs auf Kaspersky Internet Security 83

Schutzmodus wählen 83

KONTROLLE DES ZUGRIFFS AUF KASPERSKY INTERNET SECURITY.

Es kann sein, dass ein PC von mehreren Benutzern verwendet wird, deren Fertigkeiten im Umgang mit Computern völlig unterschiedlich sind. Der uneingeschränkte Zugriff der Benutzer auf Kaspersky Internet Security und dessen Einstellungen kann das Sicherheitsniveau des Computers stark beeinträchtigen.

Um den Zugriff auf das Programm zu beschränken, können Sie ein Kennwort festlegen und angeben, für welche Aktionen dieses abgefragt werden soll:

- Programmparameter ändern
- Kindersicherung aktivieren und anpassen
- Programm beenden
- Programm deinstallieren

Bewahren Sie das Kennwort für die Beschränkung der Programmdeinstallation sicher auf. Wenn Sie das Kennwort vergessen sollten, wird es schwierig sein, das Programm vom Computer zu entfernen.

Gehen Sie folgendermaßen vor, um den Zugriff auf Kaspersky Internet Security durch ein Kennwort zu beschränken:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** den Abschnitt **Allgemeine Einstellungen**.
3. Aktivieren Sie auf der rechten Fensterseite im Block **Kennwortschutz** das Kontrollkästchen **Kennwortschutz aktivieren** und klicken Sie auf **Einstellungen**.
4. Geben Sie im folgenden Fenster **Kennwortschutz** das Kennwort an und legen Sie den Bereich fest, für den die Zugriffsbeschränkung gelten soll.

SCHUTZMODUS WÄHLEN

Kaspersky Internet Security arbeitet standardmäßig im *automatischen Schutzmodus*. In diesem Modus wendet das Programm beim Auftreten gefährlicher Ereignisse automatisch die von Kaspersky Lab empfohlene Aktion an. Sie können den *interaktiven Schutzmodus* wählen, damit Kaspersky Internet Security Sie über alle gefährlichen und verdächtigen Ereignisse im System informiert und Ihnen das Programm mögliche Aktionen zur Auswahl anbietet.

Gehen Sie folgendermaßen vor, um einen Schutzmodus zu wählen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** den Abschnitt **Allgemeine Einstellungen**.
3. Deaktivieren oder aktivieren Sie im Block **Interaktiver Modus** die Kontrollkästchen für den entsprechenden Schutzmodus:
   - um den interaktiven Schutzmodus zu wählen, deaktivieren Sie das Kontrollkästchen **Aktion automatisch wählen**.
   - um den automatischen Schutzmodus zu wählen, aktivieren Sie das Kontrollkästchen **Aktion automatisch wählen**.

     Damit verdächtige Objekte bei der Arbeit im automatischen Modus nicht gelöscht werden, aktivieren Sie das Kontrollkästchen **Verdächtige Objekte nicht löschen**.

UNTERSUCHUNG DES COMPUTERS

Die Untersuchung des Computers auf Viren und Schwachstellen ist eine der wichtigsten Funktionen für die Sicherheit des Rechners. Es ist erforderlich, Ihren Computer regelmäßig auf Viren zu scannen, um die Möglichkeit der Ausbreitung schädlicher Programme auszuschließen, die nicht von den Schutzkomponenten erkannt wurden, weil beispielsweise eine zu niedrige Schutzstufe eingestellt war.

Die Aufgabe zur Schwachstellensuche umfasst eine Sicherheitsdiagnose des Betriebssystems und eine Software-Analyse zum Erkennen von Sicherheitslücken, die Angreifern zur Verbreitung schädlicher Objekte und zum Zugriff auf persönliche Daten dienen können.

Die folgenden Abschnitte informieren ausführlich über Besonderheiten und Konfiguration von Untersuchungsaufgaben sowie über Sicherheitsstufen, Methoden und Technologien für die Untersuchung.

IN DIESEM ABSCHNITT

Virensuche 84

Schwachstellensuche 92

VIRENSUCHE

Kaspersky Internet Security verfügt über folgende Aufgaben zur Virensuche:

- **Untersuchung von Objekten**. Untersuchung von Objekten, die der Benutzer festlegt. Es kann jedes beliebige der folgenden Objekte des Dateisystems auf dem Computer untersucht werden: Arbeitsspeicher, Objekte, die beim Systemstart ausgeführt werden, Systemwiederherstellung, Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzlaufwerke.
- **Vollständige Untersuchung**. Ausführliche Untersuchung des Systems. Standardmäßig werden folgende Objekte untersucht: Systemspeicher, Objekte, die beim Systemstart gestartet werden, Systemwiederherstellung, Mail-Datenbanken, Festplatten, Wechseldatenträger und Netzlaufwerke.
- **Untersuchung wichtiger Bereiche**. Virenuntersuchung der Objekte, die beim Start des Betriebssystems geladen werden.

Bei den Aufgaben zur vollständigen Untersuchung und zur Untersuchung wichtiger Bereiche handelt es sich um spezifische Aufgaben. Es wird davor gewarnt, die Liste der Untersuchungsobjekte für diese Aufgaben zu ändern.

Jede Untersuchungsaufgabe wird in einem bestimmten Bereich ausgeführt und kann nach einem festgelegten Zeitplan gestartet werden. Außerdem wird jede Untersuchungsaufgabe durch eine Sicherheitsstufe charakterisiert (Auswahl von Einstellungen für die Genauigkeit der Untersuchung). In der Grundeinstellung ist immer der Untersuchungsmodus mit Hilfe der Einträge in Datenbanken des Programms aktiviert. Außerdem können Sie verschiedene Methoden und Technologien zur Untersuchungs einsetzen s. S. 88).

Nach dem Start einer Aufgabe zur vollständigen Untersuchung oder zur Untersuchung wichtiger Bereiche wird der Untersuchungsvorgang im Abschnitt **Untersuchung** des Hauptfensters von Kaspersky Internet Security im Feld unter dem Namen der gestarteten Aufgabe angezeigt.

Beim Fund einer Bedrohung weist Kaspersky Internet Security dem gefundenen Objekt eine der folgenden Statusvarianten zu:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).
- Status *möglicherweise infiziert* (verdächtig) wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Möglicherweise enthält die Datei eine virentypische Codefolge oder den modifizierten Code eines bekannten Virus.

Anschließend zeigt das Programm eine Meldung über die gefundene Bedrohung an und führt die festgelegte Aktion aus. Sie können die Aktion beim Fund einer Bedrohung ändern.

Wenn Sie im automatischen Modus (s. Abschnitt "Schutzmodus auswählen" auf S. 83) arbeiten, dann führt Kaspersky Internet Security beim Fund gefährlicher Objekte automatisch die von den Kaspersky-Lab-Experten empfohlene Aktion aus. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, für verdächtige – **In die Quarantäne verschieben**.

Bevor ein infiziertes Objekt desinfiziert oder gelöscht wird, legt Kaspersky Internet Security eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren. Verdächtige (möglicherweise infizierte) Objekte werden in die Quarantäne verschoben. Sie können eine automatische Untersuchung der Quarantänedateien nach jedem Update festlegen.

Informationen über die Untersuchungsergebnisse und über alle Ereignisse, die bei der Aufgabenausführung auftreten, werden im Bericht von Kaspersky Internet Security protokolliert.

IN DIESEM ABSCHNITT

Sicherheitsstufe ändern und wiederherstellen 86

Zeitplan für den Untersuchungsstart erstellen 86

Liste der Untersuchungsobjekte erstellen 87

Untersuchungsmethode wählen 88

Untersuchungstechnologien wählen 88

Aktion beim Fund einer Bedrohung ändern 88

Untersuchungsstart mit den Rechten eines anderen Benutzers 89

Typ der zu untersuchenden Objekte ändern 89

Untersuchung von zusammengesetzten Dateien 90

Untersuchung optimieren 90

Wechseldatenträger beim Anschließen untersuchen 91

Verknüpfung für den Aufgabenstart erstellen 91

SICHERHEITSSTUFE ÄNDERN UND WIEDERHERSTELLEN

Sie können eine vordefinierte Sicherheitsstufe wählen, die Ihren Anforderungen entspricht, oder die Untersuchungseinstellungen entsprechend anpassen.

Während Sie eine Untersuchungsaufgabe anpassen, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Untersuchung von Objekten**).
3. Stellen Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe ein oder klicken Sie auf **Einstellungen**, um die Untersuchungseinstellungen manuell anzupassen.

Wenn manuelle Änderungen erfolgen, ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Gehen Sie folgendermaßen vor, um die empfohlenen Untersuchungseinstellungen wiederherzustellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Untersuchung von Objekten**).
3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Standard**.

ZEITPLAN FÜR DEN UNTERSUCHUNGSSTART ERSTELLEN

Es kann ein Zeitplan für den automatischen Start einer Untersuchungsaufgabe angelegt werden: In diesem werden eine Frequenz für den Aufgabenstart, ein Startzeitpunkt (falls erforderlich) sowie zusätzliche Parameter festgelegt.

Wenn der Start aus irgendeinem Grund nicht möglich war (wenn beispielsweise der Computer im betreffenden Moment ausgeschaltet war), können Sie festlegen, dass der Start einer übersprungenen Aufgabe automatisch zum nächstmöglichen Zeitpunkt erfolgt. Außerdem lässt sich festlegen, dass eine Untersuchung automatisch angehalten wird, wenn der Bildschirmschoner inaktiv oder der Computer nicht entsperrt ist. Diese Option erlaubt es, den Start einer Aufgabe zurückzustellen, bis der Benutzer seine Arbeit auf dem Computer beendet hat. Dadurch wird verhindert, dass eine Untersuchungsaufgabe Computerressourcen verbraucht, während diese für andere Aufgaben benötigt werden.

Der spezielle Modus zur Untersuchung im Computerleerlauf (s. Abschnitt "Aufgabenstart im Hintergrundmodus" auf S. 183) erlaubt es, eine Untersuchung des Arbeitsspeichers, der Systempartition und der Autostart-Objekte dann zu starten, wenn der Computer nicht verwendet wird.

Gehen Sie folgendermaßen vor, um den Startzeitplan einer Untersuchungsaufgabe anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Schwachstellensuche**).
3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan** aus und konfigurieren Sie den Startmodus für die Untersuchung.

Gehen Sie folgendermaßen vor, um den automatischen Start einer übersprungenen Aufgabe zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Schwachstellensuche**).
3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan** aus und aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**.

Gehen Sie folgendermaßen vor, damit die Untersuchung erst gestartet wird, nachdem der Benutzer seine Arbeit beendet hat:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Schwachstellensuche**).
3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan** und aktivieren Sie das Kontrollkästchen **Geplante Untersuchung anhalten, wenn Bildschirmschoner inaktiv und Computer nicht blockiert ist**.

LISTE DER UNTERSUCHUNGSOBJEKTE ERSTELLEN

Standardmäßig entspricht jeder Aufgabe zur Virensuche eine eigene Liste von Objekten. Zu diesen Objekten können sowohl Objekte des Computerdateisystems (z.B. logische Laufwerke, **Mail-Datenbanken**), als auch Objekte anderer Typen (z.B. Netzlaufwerke) gehören. Diese Liste kann geändert werden.

Wenn der Untersuchungsbereich leer ist oder kein Objekt des Untersuchungsbereichs angekreuzt wurde, kann die Untersuchungsaufgabe nicht gestartet werden.

Gehen Sie folgendermaßen vor, um für eine Untersuchungsaufgabe eine Liste der Untersuchungsobjekte zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie auf der linken Fensterseite den Abschnitt **Untersuchung**.
3. Öffnen Sie auf der rechten Fensterseite durch Klicken des Links **Auswählen** die Liste der Untersuchungsobjekte.
4. Klicken Sie im folgenden Fenster **Untersuchung** von Objekten auf **Hinzufügen**.
5. Wählen Sie im folgenden Fenster **Untersuchungsobjekt wählen ein Objekt** aus und klicken Sie auf **Hinzufügen**. Nachdem alle erforderlichen Objekte hinzugefügt wurden, klicken Sie auf **OK**. Um bestimmte Objekte aus der Untersuchungsliste auszuschließen, deaktivieren Sie die entsprechenden Kontrollkästchen.

   Dateien, die gescannt werden sollen, können auch direkt in einen speziell markierten Bereich im Abschnitt **Untersuchung** gezogen werden.

Gehen Sie folgendermaßen vor, um für die Aufgaben zur vollständigen Untersuchung, zur Untersuchung wichtiger Bereiche und zur Schwachstellensuche eine Liste mit Untersuchungsobjekten zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Untersuchungsaufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Schwachstellensuche**).

3. Klicken Sie auf der rechten Fensterseite auf **Untersuchungsobjekte**.

4. Erstellen Sie im folgenden Fenster **Untersuchungsobjekte** mit Hilfe der Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** eine Liste. Um bestimmte Objekte aus der Untersuchungsliste auszuschließen, deaktivieren Sie die entsprechenden Kontrollkästchen.

Objekte, die sich standardmäßig in der Liste befinden, können nicht geändert oder gelöscht werden.

UNTERSUCHUNGSMETHODE WÄHLEN

Bei einer Virenuntersuchung des Computers wird immer die Methode *Signaturanalyse* verwendet, bei der Kaspersky Internet Security ein gefundenes Objekt mit den Einträgen in den Datenbanken vergleicht.

Um die Effektivität der Suche zu steigern, stehen zusätzliche Untersuchungsmethoden zur Verfügung: *heuristische Analyse* (Analyse der Aktivität, die ein Objekt im System zeigt) und *Rootkit-Suche* (Utilities, die schädliche Programme im Betriebssystem verstecken).

Gehen Sie folgendermaßen vor, um die erforderlichen Untersuchungsmethoden zu verwenden:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Untersuchung von Objekten**).

3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.

4. Wählen Sie auf der Registerkarte **Erweitert** im Block **Untersuchungsmethoden** die gewünschten Parameterwerte.

UNTERSUCHUNGSTECHNOLOGIEN WÄHLEN

Neben den Untersuchungsmethoden können Sie spezielle Technologien einsetzen, mit denen das Untersuchungstempo gesteigert werden kann. Dabei werden Dateien ausgeschlossen, die seit dem letzten Scan nicht verändert wurden.

Gehen Sie folgendermaßen vor, um die Technologien zur Objektuntersuchung zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Untersuchung von Objekten**).

3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungstechnologien** die gewünschten Werte.

AKTION BEIM FUND EINER BEDROHUNG ÄNDERN

Beim Fund infizierter oder möglicherweise infizierter Objekte führt das Programm eine festgelegte Aktion aus.

Gehen Sie folgendermaßen vor, um die Aktion für gefundene Objekte zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Untersuchung von Objekten**).

3. Wählen Sie auf der rechten Fensterseite im Block **Aktion beim Fund einer Bedrohung** die entsprechende Option aus.

UNTERSUCHUNGSSTART MIT DEN RECHTEN EINES ANDEREN BENUTZERS

Die Untersuchungsaufgaben werden standardmäßig unter dem Benutzerkonto gestartet, mit dessen Rechten Sie sich im System angemeldet haben. Es kann aber erforderlich sein, eine Aufgabe mit den Rechten eines anderen Benutzers zu starten. Sie können das Benutzerkonto festlegen, mit dessen Rechten eine Untersuchungsaufgabe gestartet werden soll.

Gehen Sie folgendermaßen vor, um die Untersuchung mit den Rechten eines anderen Benutzers zu starten:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche**, **Untersuchung von Objekten** oder **Schwachstellensuche**).

3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Benutzer** das Kontrollkästchen **Aufgabe starten mit Rechten des Benutzers**. Geben Sie darunter in den Feldern den Benutzernamen und das Kennwort an.

TYP DER ZU UNTERSUCHENDEN OBJEKTE ÄNDERN

Durch die Angabe des Typs der zu untersuchenden Objekte bestimmen Sie das Format und die Größe der Dateien, die beim Ausführen der gewählten Aufgabe untersucht werden sollen.

Bei der Auswahl des Dateityps muss Folgendes beachtet werden:

- Es gibt eine Reihe von Dateiformaten (z.B. txt), für die das Risiko des Eindringens von schädlichem Code und dessen späterer Aktivierung relativ gering ist. Gleichzeitig gibt es Formate, die ausführbaren Code enthalten oder enthalten können (exe, dll, doc). Das Risiko, dass schädlicher Code in solche Dateien eindringt und aktiviert wird, ist relativ hoch.

- Ein Angreifer kann einen Virus in einer ausführbaren Datei, die in eine txt-Datei umbenannt wurde, an Ihren Computer senden. Wenn die Sie Untersuchung von Dateien nach Erweiterung gewählt haben, wird eine solche Datei bei der Untersuchung übersprungen. Wurde die Untersuchung von Dateien nach Format gewählt wurde, ignoriert Datei-Anti-Virus die Erweiterung und analysiert die Kopfzeile der Datei, wodurch sich ergeben kann, dass die Datei das Format exe besitzt. Eine solche Datei wird der sorgfältigen Virusuntersuchung unterzogen.

Gehen Sie folgendermaßen vor, um den Typ der zu untersuchenden Dateien zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Untersuchung von Objekten**).

3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Dateitypen** die gewünschte Variante.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie Archive, Datenbanken usw. Um Viren zu erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

Für jeden Typ einer zusammengesetzten Datei können Sie wählen, ob alle oder nur neue Dateien untersucht werden sollen. Verwenden Sie zur Auswahl den Link neben dem Namen des Objekts. Er verändert seinen Wert, wenn mit der linken Maustaste darauf geklickt wird. Wenn der Modus gewählt wurde, in dem nur neue und veränderte Dateien untersucht werden (s. S. 90), stehen die Links zur Auswahl aller oder nur neuer Dateien nicht zur Verfügung.

Außerdem können Sie festlegen, bis zu welcher maximalen Größe eine zusammengesetzte Datei untersucht werden soll. Zusammengesetzte Dateien, die den festgelegten Wert überschreiten, werden nicht untersucht.

Wenn umfangreiche Dateien aus Archiven extrahiert werden, erfolgt eine Untersuchung auch dann, wenn das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist.

Gehen Sie folgendermaßen vor, um Liste der zu untersuchenden zusammengesetzten Dateien zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Untersuchung von Objekten**).
3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung von zusammengesetzten Dateien** die Typen der zusammengesetzten Dateien, die untersucht werden sollen.

Gehen Sie folgendermaßen vor, um eine maximale Größe für zusammengesetzte Dateien festzulegen, die untersucht werden sollen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Untersuchung von Objekten**).
3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung von zusammengesetzten Dateien** auf die Schaltfläche **Erweitert**.
5. Aktivieren Sie im folgenden Fenster **Zusammengesetzte Dateien** das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken und legen Sie die maximale Größe für zu untersuchende Dateien fest**.

UNTERSUCHUNG OPTIMIEREN

Sie können die Untersuchungsdauer verkürzen und die Arbeitsgeschwindigkeit von Kaspersky Internet Security erhöhen. Das lässt sich erreichen, wenn nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Außerdem kann die Untersuchungsdauer für ein einzelnes Objekt beschränkt werden. Wenn eine Datei nicht innerhalb der vorgegebenen Zeit untersucht wurde, wird sie von der laufenden Untersuchung ausgeschlossen (außer Archiven und Dateien, die aus mehreren Objekten bestehen).

Gehen Sie folgendermaßen vor, damit nur neue und veränderte Dateien untersucht werden:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Untersuchung von Objekten**).

3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung optimieren** das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**.

Gehen Sie folgendermaßen vor, um die Untersuchungsdauer einzuschränken:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Untersuchung von Objekten**).

3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung optimieren** das Kontrollkästchen **Objekte überspringen, wenn Untersuchung länger als** und geben Sie die Untersuchungsdauer für eine einzelne Datei an.

WECHSELDATENTRÄGER BEIM ANSCHLIEßEN UNTERSUCHEN

In letzter Zeit treten vermehrt schädliche Objekte auf, die Schwachstellen des Betriebssystems ausnutzen, um sich über lokale Netzwerke und Wechseldatenträger auszubreiten. Kaspersky Internet Security bietet eine Funktion, mit der Wechseldatenträger untersucht werden können, wenn sie an den Computer angeschlossen werden.

Gehen Sie folgendermaßen vor, um die Funktion anzupassen, mit der Wechseldatenträger untersucht werden, wenn sie an den Computer angeschlossen werden:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite unter **Untersuchung des Computers** den Abschnitt **Allgemeine Einstellungen**.

3. Wählen Sie im Block **Wechseldatenträger beim Anschließen untersuchen** eine Aktion und begrenzen Sie bei Bedarf im Feld unten die Größe der zu untersuchenden Laufwerke.

VERKNÜPFUNG FÜR DEN AUFGABENSTART ERSTELLEN

Für den Schnellstart der Aufgaben zur vollständigen und schnellen Untersuchung sowie zur Schwachstellensuche ist im Programm die Möglichkeit vorgesehen, Verknüpfungen anzulegen. So kann die erforderliche Untersuchungsaufgabe gestartet werden, ohne das Programmhauptfenster oder das Kontextmenü zu öffnen.

Gehen Sie folgendermaßen vor, um eine Verknüpfung für den Start einer Untersuchungsaufgabe zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite unter **Untersuchung des Computers** den Abschnitt **Allgemeine Einstellungen**.

3. Klicken Sie auf der rechten Seite des Fensters im Block **Schneller Aufgabenstart** neben dem entsprechenden Aufgabennamen (**Untersuchung wichtiger Bereiche**, **Vollständige Untersuchung** oder **Schwachstellensuche**) auf **Verknüpfung erstellen**.

4. Geben Sie im folgenden Fenster an, wo und unter welchem Namen die Verknüpfung gespeichert werden soll. Standardmäßig wird die Verknüpfung unter dem Aufgabennamen im Ordner *Arbeitsplatz* des aktiven Computerbenutzers erstellt.

SUCHE NACH SCHWACHSTELLEN

Schwachstellen in einem Betriebssystem können auf Programmierungs- oder Organisationsfehler, unsichere Kennwörter, Malware-Aktionen u.a. zurückgehen. Im Rahmen der Schwachstellensuche wird das System analysiert und es wird in den Einstellungen des Betriebssystems und des Browsers nach Anomalien und Beschädigungen gesucht. Weiterhin findet eine Suche nach Schwachstellen bei den Diensten statt und es werden andere Schutzmaßnahmen getroffen.

Die Diagnose kann eine gewisse Zeit beanspruchen. Anschließend werden die gefundenen Probleme im Hinblick auf ihre Gefährlichkeit für das System analysiert.

Nach dem Start der Aufgabe zur Schwachstellensuche (s. S. 66) wird der Vorgang im Fenster **Schwachstellensuche** im Feld **Ende** angezeigt. Die bei der Untersuchung im System und in Programmen gefundenen Schwachstellen werden im gleichen Fenster auf den Registerkarten **Systemschwachstellen** und **Programme mit Schwachstellen** angezeigt.

Während die Virensuche ausgeführt wird, werden Informationen über ihre Ergebnisse im Bericht von Kaspersky Internet Security aufgezeichnet.

Wie für die Untersuchungsaufgaben kann auch für die Aufgabe zur Schwachstellensuche ein Startzeitplan erstellt, eine Liste der Untersuchungsobjekte angelegt (s. S. 87), ein Benutzerkonto gewählt (s. Abschnitt "Untersuchungsstart mit den Rechten eines anderen Benutzers" aud S. 89) und eine Verknüpfung für den schnellen Aufgabenstart erstellt werden. In der Grundeinstellung sind die auf dem Computer installierten Anwendungen als Untersuchungsobjekt gewählt.

UPDATE

Das Update der Datenbanken und Programm-Module von Kaspersky Internet Security gewährleistet den aktuellen Zustand Ihres Computerschutzes. Jeden Tag tauchen neue Viren, trojanische Programme und andere Malware auf. Informationen über Bedrohungen und entsprechende Neutralisierungsmethoden sind in den Datenbanken von Kaspersky Internet Security enthalten. Deshalb stellt die regelmäßige Aktualisierung des Programms einen sehr wichtigen Faktor für die Sicherheit Ihres Computers und die rechtzeitige Erkennung neuer Gefahren dar.

Für ein regelmäßiges Update ist eine gültige Programmlizenz erforderlich. Ohne Lizenz ist nur ein einmaliges Update möglich.

Die Aktualisierung des Programms umfasst den Download und die Installation folgender Elemente auf Ihren Computer:

- Datenbanken für Kaspersky Internet Security.

  Der Schutz der Informationen auf ihrem Computer basiert auf Datenbanken, die Beschreibungen von Bedrohungssignaturen und Netzwerkangriffen, sowie entsprechende Desinfektionsmethoden enthalten. Die Schutzkomponenten verwenden diese bei der Suche und Desinfektion gefährlicher Objekte auf Ihrem Computer. Die Datenbanken werden regelmäßig durch Einträge über neue Bedrohungen und entsprechende Desinfektionsmethoden ergänzt. Deshalb wird ausdrücklich empfohlen, die Datenbanken regelmäßig zu aktualisieren.

  Gemeinsam mit den Datenbanken von Kaspersky Internet Security werden auch die Netzwerktreiber aktualisiert, die die Funktionalität für das Abfangen des Netzwerkverkehrs durch die Schutzkomponenten gewährleisten.

- Programm-Module.

  Neben den Datenbanken von Kaspersky Internet Security können auch die Programm-Module aktualisiert werden. Updatepakete beheben Schwachstellen von Kaspersky Internet Security, fügen neue Funktionen hinzu und optimieren bestehende Funktionen.

Die wichtigste Updatequelle für Kaspersky Internet Security sind spezielle Updateserver von Kaspersky Lab. Parallel zur Aktualisierung von Kaspersky Internet Security können Sie die Updates für Datenbanken und Programm-Module, die von den Kaspersky-Lab-Servern heruntergeladen werden, in einen lokalen Ordner kopieren, auf den dann andere Netzwerkcomputer zugreifen können. Dadurch lässt sich Internet-Traffic einsparen.

Zusätzlich kann die Parameter für den automatischen Start des Updates angepasst werden.

Um Updates erfolgreich von den Servern herunterzuladen, muss Ihr Computer mit dem Internet verbunden sein. In der Grundeinstellung wird die Internetverbindung automatisch ermittelt. Wenn Sie einen Proxyserver verwenden, kann es notwendig sein, die Parameter der Verbindung anzupassen.

Bei der Aktualisierung werden die auf Ihrem Computer installierten Programm-Module und Datenbanken mit der aktuellen Version in der Updatequelle verglichen (s. S. 142). Wenn Datenbanken und Module nicht aktuell sind, werden fehlende Teile der Updates auf Ihrem Computer installiert.

Wenn die Datenbanken stark veraltet sind, kann das Updatepaket relativ umfangreich sein und zusätzlichen Internet-Datenverkehr verursachen (bis zu mehreren Dutzend Megabyte).

Bevor die Datenbanken aktualisiert werden, legt Kaspersky Internet Security eine Sicherungskopie an. Bei Bedarf können Sie zur vorhergehenden Version der Datenbanken zurückkehren.

Informationen über den aktuellen Status der Datenbanken von Kaspersky Internet Security werden im Abschnitt **Update** des Programmhauptfensters angezeigt.

Informationen über die Updateergebnisse und über alle Ereignisse, die bei der Ausführung einer Updateaufgabe auftreten, werden im Bericht von Kaspersky Internet Security protokolliert.

IN DIESEM ABSCHNITT

Updatequelle wählen 93

Zeitplan für Updatestart erstellen 95

Rollback zum vorherigen Update 96

Untersuchung der Quarantäne nach dem Update 96

Proxyserver verwenden 96

Updatestart mit den Rechten eines anderen Benutzers 97

UPDATEQUELLE AUSWÄHLEN

Eine *Updatequelle* ist eine Ressource, die Updates der Datenbanken und der Module für Kaspersky Internet Security enthält. Als Updatequelle können HTTP- oder FTP-Server, lokale Ordner oder Netzwerkordner angegebenen werden.

Als primäre Updatequelle dienen die Kaspersky-Lab-Updateserver, auf denen Updates der Datenbanken und Programm-Module für alle Kaspersky-Lab-Produkte zur Verfügung gestellt werden.

Wenn Sie keinen Zugriff auf die Kaspersky-Lab-Updateserver besitzen (wenn beispielsweise der Internetzugang eingeschränkt ist), können Sie sich an unsere Zentrale (http://www.kaspersky.de/kontakt) wenden. Dort können Sie die Adressen der Partner von Kaspersky Lab erfahren, die Ihnen die Updates auf einem Wechseldatenträger anbieten können.

Geben Sie zur Bestellung von Updates auf Wechseldatenträgern unbedingt an, ob Sie Updates für die Programm-Module erhalten möchten.

In der Grundeinstellung enthält die Liste nur die Kaspersky-Lab-Updateserver. Wenn mehrere Ressourcen als Updatequellen gewählt wurden, greift Kaspersky Internet Security bei der Aktualisierung genau nach der Liste darauf zu und aktualisiert sich von der ersten verfügbaren Quelle.

Wenn Sie als Updatequelle eine Ressource gewählt haben, die sich außerhalb des lokalen Netzwerks befindet, ist für die Aktualisierung eine Internetverbindung erforderlich.

Gehen Sie folgendermaßen vor, um eine Updatequelle auszuwählen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Updateparameter**.
3. Klicken Sie auf der rechten Fensterseite auf **Updatequelle**.
4. Öffnen Sie im folgenden Fenster auf der Registerkarte **Quelle** das Auswahlfenster. Klicken Sie dazu auf die Schaltfläche **Hinzufügen**.
5. Wählen Sie im folgenden Fenster **Updatequelle wählen** den Ordner, der die Updates enthält, oder geben Sie im Feld **Quelle** die Adresse des Servers ein, von dem die Updates heruntergeladen werden sollen.

REGION DES UPDATESERVERS WÄHLEN

Wenn Sie die Kaspersky-Lab-Server als Updatequelle verwenden, kann der für Sie günstigste Serverstandort für den Update-Download gewählt werden. Kaspersky Lab verfügt in mehreren Ländern der Erde über Server.

Durch die Verwendung des geografisch am nächsten gelegenen Kaspersky-Lab-Updateservers kann sich die Dauer des Update-Downloads verkürzen und das Übertragungstempo erhöhen. In der Grundeinstellung werden Informationen über den aktuellen Standort aus der Registrierung des Betriebssystems verwendet. Sie können die Region manuell wählen.

Gehen Sie folgendermaßen vor, um die Region des Servers zu wählen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Updateparameter**.
3. Klicken Sie auf der rechten Fensterseite auf **Updatequelle**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Quelle** im Block **Regionsoptionen** die Variante **Aus der Liste wählen**und wählen Sie aus der Dropdown-Liste das Land aus, in dem Sie sich gegenwärtig aufhalten.

UPDATE AUS DEM GEMEINSAMEN ORDNER

Um Internet-Datenverkehr einzusparen, kann festgelegt werden, dass Kaspersky Internet Security auf den Netzwerkcomputern aus einem gemeinsamen Ordner aktualisiert werden soll. In diesem Fall lädt ein Computer des Netzwerks das Updatepaket von den Kaspersky-Lab-Servern im Internet oder von einer anderen Webressource, auf der sich die aktuellen Updates befinden, herunter. Die heruntergeladenen Updates werden in einem gemeinsamen Ordner abgelegt, auf den die anderen Netzwerkcomputer zugreifen, um die Updates für Kaspersky Internet Security zu erhalten.

Gehen Sie folgendermaßen vor, um den Modus für die Update-Verteilung zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Updateparameter**.
3. Aktivieren Sie im Block **Erweitert** das Kontrollkästchen **Updates in folgenden Ordner kopieren** und geben Sie darunter im Feld den Pfad des gemeinsamen Ordners an, in dem heruntergeladene Updates abgelegt werden sollen. Außerdem kann mit Hilfe der Schaltfläche **Durchsuchen** ein Ordner gewählt werden.

Gehen Sie folgendermaßen vor, damit der Computer aus dem gewählten gemeinsamen Ordner aktualisiert wird:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Updateparameter**.

3. Klicken Sie auf der rechten Fensterseite auf **Updatequelle**.

4. Öffnen Sie im folgenden Fenster auf der Registerkarte **Quelle** das Auswahlfenster. Klicken Sie dazu auf die Schaltfläche **Hinzufügen**.

5. Wählen Sie im folgenden Fenster **Updatequelle wählen** einen Ordner oder geben im Feld **Quelle** den vollständigen Pfad an.

6. Deaktivieren Sie auf der Registerkarte **Quelle** das Kontrollkästchen **Kaspersky-Lab-Updateserver**.

ZEITPLAN FÜR UPDATESTART ERSTELLEN

Es kann ein Zeitplan für den automatischen Start einer Updateaufgabe angelegt werden: In diesem werden eine Frequenz für den Aufgabenstart, ein Startzeitpunkt (falls erforderlich) sowie zusätzliche Parameter festgelegt.

Wenn der Aufgabenstart aus irgendeinem Grund nicht möglich war (wenn beispielsweise der Computer im betreffenden Moment ausgeschaltet war), können Sie festlegen, dass der Start einer übersprungenen Aufgabe automatisch zum nächstmöglichen Zeitpunkt erfolgt.

Außerdem können Sie den automatischen Aufgabenstart nach dem Start des Programms aufschieben. Dann werden alle geplanten Aufgaben erst gestartet, nachdem Kaspersky Internet Security gestartet wurde und eine bestimmte Zeit verstrichen ist.

Der spezielle Modus zur Untersuchung im Computerleerlauf (s. Abschnitt "Aufgabenstart im Hintergrundmodus" auf S. 183) erlaubt es, ein automatisches Update dann zu starten, wenn der Computer nicht verwendet wird.

- *Gehen Sie folgendermaßen vor, um den Startzeitplan für die Updateaufgabe anzupassen:*

  1. Öffnen Sie das Programmkonfigurationsfenster.

  2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Updateparameter**.

  3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.

  4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan**aus und konfigurieren Sie den Startmodus für die Aktualisierung.

- *Gehen Sie folgendermaßen vor, um den automatischen Start einer übersprungenen Aufgabe zu aktivieren:*

  1. Öffnen Sie das Programmkonfigurationsfenster.

  2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Updateparameter**.

  3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.

  4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan** aus und aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**.

- *Gehen Sie folgendermaßen vor, um den Aufgabenstart nach dem Programmstart aufzuschieben:*

  1. Öffnen Sie das Programmkonfigurationsfenster.

  2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Updateparameter**.

  3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.

  4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan** aus und legen Sie im Feld **Start nach Programmstart aufschieben für** fest, wie lange der Aufgabenstart zurückgestellt werden soll.

ROLLBACK ZUM VORHERIGEN UPDATE

Nach dem ersten Update der Datenbanken und der Programm-Module von Kaspersky Internet Security steht Ihnen die Funktion des Rollback zu den Vorversionen der Datenbanken zur Verfügung.

Jedes Mal, wenn Sie das Update starten, erstellt Kaspersky Internet Security zuerst eine Sicherungskopie der bisher verwendeten Datenbanken und Programm-Module und beginnt danach mit der Aktualisierung. Dadurch wird Ihnen erlaubt, bei Bedarf zur Verwendung der vorherigen Datenbanken zurückzukehren. Die Rollback-Funktion ist beispielsweise nützlich, wenn die neue Datenbankversion eine fehlerhafte Signatur enthält, die dazu führt, dass Kaspersky Internet Security ein harmloses Programm blockiert.

Wenn die Datenbanken von Kaspersky Internet Security beschädigt sind, wird empfohlen, die Updateaufgabe zu starten, um funktionsfähige aktuelle Datenbanken herunterzuladen.

- *Gehen Sie folgendermaßen vor, um zur Verwendung der vorhergehenden Version der Datenbanken zurückzukehren:*

  1. Öffnen Sie das Programmhauptfenster.
  2. Wählen Sie auf der linken Fensterseite den Abschnitt **Update**.
  3. Klicken Sie auf der rechten Fensterseite auf **Rollback zu den vorherigen Datenbanken**.

UNTERSUCHUNG DER QUARANTÄNE NACH DEM UPDATE

Wenn sich bei der Untersuchung nicht genau ermitteln lässt, von welchen Schadprogrammen ein Objekt infiziert ist, wird es in die Quarantäne verschoben. Eine Bedrohung kann möglicherweise eindeutig bestimmt und desinfiziert werden, nachdem die Datenbanken aktualisiert wurden. Sie können eine automatische Untersuchung der Quarantäneobjekte nach jedem Update festlegen.

Es wird empfohlen, die Objekte in der Quarantäne regelmäßig zu überprüfen. Aufgrund der Untersuchung kann sich ihr Status ändern. Bestimmte Objekte können am ursprünglichen Ort wiederhergestellt und wieder verwendet werden.

- *Gehen Sie folgendermaßen vor, um festzulegen, dass die Quarantänedateien nach einem Update automatisch untersucht werden:*

  1. Öffnen Sie das Programmkonfigurationsfenster.
  2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Updateparameter**.
  3. Aktivieren Sie im Block **Erweitert** das Kontrollkästchen **Quarantänedateien nach jedem Update untersuchen**.

PROXYSERVER VERWENDEN

Wenn die Internetverbindung über einen Proxyserver erfolgt, müssen seine Parameter angepasst werden, um eine korrekte Aktualisierung von Kaspersky Internet Security zu ermöglichen.

- *Gehen Sie folgendermaßen vor, um die Proxyserver-Parameter anzupassen:*

  1. Öffnen Sie das Programmkonfigurationsfenster.
  2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Updateparameter**.
  3. Klicken Sie auf der rechten Fensterseite auf **Updatequelle**.
  4. Klicken Sie im folgenden Fenster auf der Registerkarte **Quelle** auf die Schaltfläche **Proxyserver**.

5. Passen Sie im folgenden Fenster **Proxyserver-Einstellungen** die Parameter für den Proxyserver an.

UPDATESTART MIT DEN RECHTEN EINES ANDEREN BENUTZERS

Das Update wird standardmäßig unter dem Benutzerkonto gestartet, mit dessen Rechten Sie sich im System angemeldet haben. Das Update für Kaspersky Internet Security kann aber auch aus einer Quelle erfolgen, auf die Sie keinen Zugriff besitzen (z.B. Netzwerkordner, der Updates enthält) oder für die Sie nicht über Rechte eines autorisierten Benutzers für den Proxyserver verfügen. Sie können das Update von Kaspersky Internet Security unter dem Namen eines Benutzers starten, der über die erforderlichen Privilegien verfügt.

➧ *Gehen Sie folgendermaßen vor, um das Update mit den Rechten eines anderen Benutzers zu starten:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Updateparameter**.
3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Benutzer** das Kontrollkästchen **Aufgabe starten mit Rechten des Benutzers**. Geben Sie darunter in den Feldern den Benutzernamen und das Kennwort an.

DATEI-ANTI-VIRUS

Datei-Anti-Virus schützt das Dateisystem des Computers vor einer Infektion. Die Komponente wird beim Hochfahren des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die auf Ihrem Computer und auf allen angeschlossenen Laufwerken geöffnet, gespeichert und gestartet werden.

Sie können einen Schutzbereich anlegen und eine Sicherheitsstufe (Auswahl von Einstellungen für die Untersuchungsgenauigkeit) wählen.

Wenn ein Benutzer oder ein Programm auf eine Datei zugreift, prüft Datei-Anti-Virus, ob die Datenbanken iChecker und iSwift Informationen über die Datei enthalten, und entscheidet auf Basis dieser Informationen, ob eine Untersuchung der Datei erforderlich ist.

In der Grundeinstellung ist immer der Untersuchungsmodus mit Hilfe der Einträge in Datenbanken des Programms aktiviert. Außerdem können heuristische Analyse (s. S. 101) und unterschiedliche Untersuchungstechnologien (s. S. 101) eingesetzt werden.

Beim Fund einer Bedrohung weist Kaspersky Internet Security dem gefundenen Objekt eine der folgenden Statusvarianten zu:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).
- Status *möglicherweise infiziert* (verdächtig) wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Möglicherweise enthält die Datei eine virentypische Codefolge oder den modifizierten Code eines bekannten Virus.

Anschließend zeigt das Programm auf dem Bildschirm eine Meldung über die gefundene Bedrohung an und führt die festgelegte Aktion aus. Sie können die Aktion beim Fund einer Bedrohung ändern.

Wenn Sie im automatischen Modus (s. Abschnitt "Schutzmodus auswählen" auf S. 83) arbeiten, dann führt Kaspersky Internet Security beim Fund gefährlicher Objekte automatisch die von den Kaspersky-Lab-Experten empfohlene Aktion aus. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, für verdächtige – **In die Quarantäne verschieben**.

Bevor ein infiziertes Objekt desinfiziert oder gelöscht wird, legt Kaspersky Internet Security eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren. Verdächtige

(möglicherweise infizierte) Objekte werden in die Quarantäne verschoben. Sie können eine automatische Untersuchung der Quarantänedateien nach jedem Update festlegen.

IN DIESEM ABSCHNITT

Datei-Anti-Virus aktivieren und deaktivieren 98

Datei-Anti-Virus automatisch anhalten 98

Schutzbereich festlegen 99

Sicherheitsstufe ändern und wiederherstellen 100

Untersuchungsmodus wählen 100

Heuristische Analyse verwenden 101

Untersuchungstechnologien wählen 101

Aktion für gefundene Objekte ändern 101

Untersuchung von zusammengesetzten Dateien 102

Untersuchung optimieren 103

DATEI-ANTI-VIRUS AKTIVIEREN UND DEAKTIVIEREN

Datei-Anti-Virus ist standardmäßig aktiviert und arbeitet im optimalen Modus. Bei Bedarf kann Datei-Anti-Virus deaktiviert werden.

Gehen Sie folgendermaßen vor, um Datei-Anti-Virus zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Datei-Anti-Virus aktivieren**.

DATEI-ANTI-VIRUS AUTOMATISCH ANHALTEN

Bei der Ausführung von Arbeiten, die die Betriebssystemressourcen stark beanspruchen, kann die Arbeit von Datei-Anti-Virus vorübergehend angehalten werden. Um die Belastung zu verringern und den schnellen Zugriff auf Objekte zu gewährleisten, kann festgelegt werden, dass die Komponente zu einem bestimmten Zeitpunkt oder bei der Arbeit mit bestimmten Programmen automatisch angehalten wird.

Das Anhalten von Datei-Anti-Virus bei einem Konflikt mit bestimmten Programmen gilt als Notlösung! Sollten bei der Arbeit der Komponente Konflikte auftreten, dann wenden Sie sich an den Technischen Support von Kaspersky Lab (http://support.kaspersky.de). Die Spezialisten helfen Ihnen dabei, auf Ihrem Computer die gemeinsame Arbeit von Kaspersky Internet Security mit anderen Programmen einzurichten.

Gehen Sie folgendermaßen vor, damit die Komponente zu einem bestimmten Zeitpunkt angehalten wird:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Aufgabe anhalten** das Kontrollkästchen **Nach Zeitplan** und klicken Sie auf **Zeitplan**.

5. Geben Sie im Fenster **Aufgabe anhalten** in den Feldern **Anhalten um** und **Fortsetzen um** den erforderlichen Zeitraum an (im Format HH:MM).

Gehen Sie folgendermaßen vor, damit die Komponente beim Start bestimmter Programme angehalten wird:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.

3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Aufgabe anhalten** das Kontrollkästchen **Bei Programmstart** und klicken Sie auf die Schaltfläche **Auswählen**.

5. Legen Sie im Fenster **Programme** die Liste der Programme an, bei deren Arbeit die Komponente angehalten werden soll.

SCHUTZBEREICH FESTLEGEN

Der Begriff Schutzbereich umfasst den Ort der Untersuchungsobjekte und den Typ der zu untersuchenden Dateien. Kaspersky Internet Security untersucht standardmäßig nur potentiell infizierbare Dateien, die von beliebigen Festplatten, Wechseldatenträgern und Netzlaufwerken aus gestartet werden.

Sie können den Schutzbereich erweitern oder einschränken, indem Sie Untersuchungsobjekte hinzufügen / entfernen oder den Typ der zu untersuchenden Dateien ändern. Es können beispielsweise nur exe-Dateien, die von Netzlaufwerken aus gestartet werden, zur Untersuchung gewählt werden.

Bei der Auswahl des Dateityps muss Folgendes beachtet werden:

- Es gibt eine Reihe von Dateiformaten (z.B. txt), für die das Risiko des Eindringens von schädlichem Code und dessen späterer Aktivierung relativ gering ist. Gleichzeitig gibt es Formate, die ausführbaren Code enthalten oder enthalten können (exe, dll, doc). Das Risiko, dass schädlicher Code in solche Dateien eindringt und aktiviert wird, ist relativ hoch.

- Ein Angreifer kann einen Virus in einer ausführbaren Datei, die in eine txt-Datei umbenannt wurde, an Ihren Computer senden. Wenn die Sie Untersuchung von Dateien nach Erweiterung gewählt haben, wird eine solche Datei bei der Untersuchung übersprungen. Wurde die Untersuchung von Dateien nach Format gewählt wurde, ignoriert Datei-Anti-Virus die Erweiterung und analysiert die Kopfzeile der Datei, wodurch sich ergeben kann, dass die Datei das Format exe besitzt. Eine solche Datei wird der sorgfältigen Virusuntersuchung unterzogen.

Gehen Sie folgendermaßen vor, um die Liste der Untersuchungsobjekte zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

4. Öffnen Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Schutzbereich** das Fenster zur Objektauswahl. Klicken Sie dazu auf den Link **Hinzufügen**.

5. Wählen Sie im Fenster **Untersuchungsobjekt wählen** ein Objekt aus und klicken Sie auf die Schaltfläche **Hinzufügen**.

6. Nachdem alle erforderlichen Objekte hinzugefügt wurden, klicken Sie im Fenster **Untersuchungsobjekt wählen** auf **OK**.

7. Um ein Objekt aus der Untersuchungsliste auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

Gehen Sie folgendermaßen vor, um den Typ der zu untersuchenden Dateien zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Wählen Sie auf der Registerkarte **Allgemein** im Block **Dateitypen** den gewünschten Parameter.

SICHERHEITSSTUFE ÄNDERN UND WIEDERHERSTELLEN

Abhängig von den aktuellen Erfordernissen können Sie eine vordefinierte Stufe für die Sicherheit von Dateien und Speicher wählen oder die Einstellungen von Datei-Anti-Virus entsprechend anpassen.

Während der Konfiguration von Datei-Anti-Virus können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese Einstellungen gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und entsprechen der Sicherheitsstufe **Empfohlen**.

Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe für Dateien und Speicher zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Stellen Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe ein oder klicken Sie auf **Einstellungen**, um die Untersuchungseinstellungen manuell anzupassen.

   Wenn manuelle Änderungen erfolgen, ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Gehen Sie folgendermaßen vor, um die standardmäßigen Schutzeinstellungen wiederherzustellen,

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Standard**.

UNTERSUCHUNGSMODUS WÄHLEN

Unter Untersuchungsmodus wird die Bedingung für das Auslösen von Datei-Anti-Virus verstanden. In der Grundeinstellung verwendet Kaspersky Internet Security den intelligenten Modus, in dem die Entscheidung über die Untersuchung eines Objekts auf Basis der Operationen, die damit ausgeführt werden sollen, gefällt wird. Beispielsweise untersucht Kaspersky Internet Security bei der Arbeit mit einem Microsoft Office-Dokument eine Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.

Sie können den Untersuchungsmodus für Objekte ändern. Der passende Modus ist davon abhängig, mit welcher Art von Dateien Sie überwiegend arbeiten.

Gehen Sie folgendermaßen vor, um den Untersuchungsmodus für Objekte zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungsmodus** den erforderlichen Modus.

HEURISTISCHE ANALYSE VERWENDEN

Bei der Arbeit von Datei-Anti-Virus wird immer die Methode *Signaturanalyse* verwendet, bei der Kaspersky Internet Security ein gefundenes Objekt mit den Einträgen in den Datenbanken vergleicht.

Um die Effektivität des Schutzes zu steigern, können Sie eine *heuristische Analyse* verwenden (Analyse der Aktivität, die ein Objekt im System zeigt). Diese Analyse erlaubt die Erkennung neuer Schadobjekte, über die noch keine Datenbankeinträge vorliegen.

- *Gehen Sie folgendermaßen vor, um die Verwendung der heuristischen Analyse zu aktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster **Leistung** im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse** und stellen Sie darunter die Genauigkeitsstufe der Untersuchung ein.

UNTERSUCHUNGSTECHNOLOGIEN WÄHLEN

Zusätzlich zur heuristischen Analyse können Sie spezielle Technologien einsetzen, mit denen das Tempo der Objektuntersuchung gesteigert werden kann. Dabei werden Dateien ausgeschlossen, die seit dem letzten Scan nicht verändert wurden.

- *Gehen Sie folgendermaßen vor, um die Technologien zur Objektuntersuchung zu aktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungstechnologien** die gewünschten Werte.

AKTION FÜR GEFUNDENE OBJEKTE ÄNDERN

Beim Fund infizierter oder möglicherweise infizierter Objekte führt das Programm eine festgelegte Aktion aus.

- *Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Wählen Sie auf der rechten Fensterseite im Block **Aktion beim Fund einer Bedrohung** die entsprechende Option aus.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie Archive, Datenbanken usw. Um Viren zu erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

Für jeden Typ einer zusammengesetzten Datei können Sie wählen, ob alle oder nur neue Dateien untersucht werden sollen. Verwenden Sie zur Auswahl den Link neben dem Namen des Objekts. Er verändert seinen Wert, wenn mit der linken Maustaste darauf geklickt wird. Wenn der Modus gewählt wurde, in dem nur neue und veränderte Dateien untersucht werden (s. S. 103), stehen die Links zur Auswahl aller oder nur neuer Dateien nicht zur Verfügung.

In der Grundeinstellung untersucht Kaspersky Internet Security nur angehängte OLE-Objekte.

Bei der Untersuchung von umfangreichen zusammengesetzten Dateien kann das vorausgehende Entpacken viel Zeit beanspruchen. Diese Dauer kann reduziert werden, wenn die Untersuchung von Dateien, die eine bestimmte Größe überschreiten, im Hintergrundmodus erfolgt. Wenn bei der Arbeit mit einer solchen Datei ein schädliches Objekt gefunden wird, werden Sie von Kaspersky Internet Security darüber informiert.

Außerdem können Sie festlegen, bis zu welcher maximalen Größe eine zusammengesetzte Datei untersucht werden soll. Zusammengesetzte Dateien, die den festgelegten Wert überschreiten, werden nicht untersucht.

Wenn umfangreiche Dateien aus Archiven extrahiert werden, erfolgt eine Untersuchung auch dann, wenn das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist.

Gehen Sie folgendermaßen vor, um Liste der zu untersuchenden zusammengesetzten Dateien zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung von zusammengesetzten Dateien** die Typen der zusammengesetzten Dateien, die untersucht werden sollen.

Gehen Sie folgendermaßen vor, um eine maximale Größe für zusammengesetzte Dateien festzulegen, die untersucht werden sollen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung von zusammengesetzten Dateien** auf die Schaltfläche **Erweitert**.
5. Aktivieren Sie im Fenster **Zusammengesetzte Dateien** das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** und legen Sie eine maximale Größe für zu untersuchende Dateien fest.

Gehen Sie folgendermaßen vor, damit umfangreiche zusammengesetzte Dateien im Hintergrundmodus entpackt werden:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung von zusammengesetzten Dateien** auf die Schaltfläche **Erweitert**.

5. Aktivieren Sie im Fenster **Zusammengesetzte Dateien** das Kontrollkästchen **Zusammengesetzte Dateien im Hintergrund entpacken** und legen Sie eine minimale Dateigröße fest.

UNTERSUCHUNG OPTIMIEREN

Sie können die Untersuchungsdauer verkürzen und die Arbeitsgeschwindigkeit von Kaspersky Internet Security erhöhen. Das lässt sich erreichen, wenn nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Gehen Sie folgendermaßen vor, damit nur neue und veränderte Dateien untersucht werden:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung optimieren** das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**.

MAIL-ANTI-VIRUS

Mail-Anti-Virus untersucht, ob in ein- und ausgehenden E-Mails gefährliche Objekte vorhanden sind. Diese Komponente wird beim Start des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle E-Mail-Nachrichten, die über die Protokolle POP3, SMTP, IMAP, MAPI und NNTP sowie über geschützte Verbindungen (SSL) über die Protokolle POP3 und IMAP übertragen werden (s. Abschnitt "Untersuchung geschützter Verbindungen" auf S. 139)..

Als Indikator für die Arbeit der Komponente dient das Symbol im Infobereich der Taskleiste, das jedes Mal bei der Untersuchung einer E-Mail das Aussehen annimmt.

Sie können die Nachrichtentypen angeben, die untersucht werden sollen, und eine Sicherheitsstufe (s. S. 105) wählen (Auswahl von Einstellungen für die Untersuchungsgenauigkeit).

Jede Nachricht, die von einem Benutzer empfangen oder gesendet wird, wird abgefangen und in ihre Bestandteile (Kopfzeile, Briefkörper, Anhänge) zerlegt. Der Briefkörper und die Anhänge einer Nachricht (einschließlich eingebetteten OLE-Objekten) werden auf Bedrohungen untersucht.

In der Grundeinstellung ist immer der Untersuchungsmodus mit Hilfe der Einträge in Datenbanken des Programms aktiviert. Zusätzlich kann die heuristische Analyse eingesetzt werden. Außerdem können Sie die Anlagenfilterung (s. S. 106) aktivieren, mit der Dateien bestimmter Typen automatisch umbenannt oder gelöscht werden können.

Beim Fund einer Bedrohung weist Kaspersky Internet Security dem gefundenen Objekt eine der folgenden Statusvarianten zu:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).
- Status *möglicherweise infiziert* (verdächtig) wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Möglicherweise enthält die Datei eine virentypische Codefolge oder den modifizierten Code eines bekannten Virus.

Anschließend blockiert das Programm die Nachricht, zeigt auf dem Bildschirm eine Meldung über die gefundene Bedrohung an und führt die festgelegte Aktion aus. Sie können die Aktion beim Fund einer Bedrohung ändern (s. Abschnitt "Aktion für gefundene Objekte ändern" auf S. 106).

Wenn Sie im automatischen Modus (s. Abschnitt "Schutzmodus auswählen" auf S. 83) arbeiten, dann führt Kaspersky Internet Security beim Fund gefährlicher Objekte automatisch die von den Kaspersky-Lab-Experten empfohlene Aktion aus. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, für verdächtige – **In die Quarantäne verschieben**.

Bevor ein infiziertes Objekt desinfiziert oder gelöscht wird, legt Kaspersky Internet Security eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren. Verdächtige (möglicherweise infizierte) Objekte werden in die Quarantäne verschoben. Sie können eine automatische Untersuchung der Quarantänedateien nach jedem Update festlegen.

Bei erfolgreicher Desinfektion erhält der Benutzer Zugriff auf die E-Mail. Wenn die Desinfektion fehlschlägt, wird das infizierte Objekt aus der Nachricht gelöscht. Als Ergebnis der Antiviren-Bearbeitung wird in die Betreffzeile der E-Mail ein spezieller Text eingefügt, der darüber informiert, dass sie von Kaspersky Internet Security bearbeitet wurde.

Für das Mailprogramm Microsoft Office Outlook ist ein integrierbares Erweiterungsmodul (s. Abschnitt "E-Mail-Untersuchung in Microsoft Office Outlook" auf S. 107) vorgesehen, das die Feineinstellung der E-Mail-Untersuchung erlaubt.

Wenn Sie das Mailprogramm The Bat! verwenden, kann Kaspersky Internet Security zusammen mit anderen Antiviren-Anwendungen benutzt werden. Dabei werden die Regeln zur Verarbeitung des Mailverkehrs (s. Abschnitt "E-Mail-Untersuchung in The Bat!" auf S. 107) direkt im Programm The Bat! erstellt und besitzen Vorrang gegenüber den Parametern für den E-Mail-Schutz des Programms.

Bei der Arbeit mit anderen Mailprogrammen (einschließlich Microsoft Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, Incredimail) untersucht Mail-Anti-Virus den Mailverkehr der Protokolle SMTP, POP3, IMAP und NNTP bei Empfang bzw. Versand.

Beachten Sie, dass bei der Arbeit mit dem Mailprogramm Thunderbird E-Mails, die mit dem IMAP- Protokoll übertragen werden, nicht auf Viren untersucht werden, wenn Filter verwendet werden, die Nachrichten aus dem Ordner **Posteingang** verschieben.

IN DIESEM ABSCHNITT

Mail-Anti-Virus aktivieren und deaktivieren 104

Schutzbereich festlegen 105

Sicherheitsstufe ändern und wiederherstellen..... 105

Heuristische Analyse verwenden 106

Aktion für gefundene Objekte ändern 106

Anlagenfilterung 106

Untersuchung von zusammengesetzten Dateien 107

E-Mail-Untersuchung in Microsoft Office Outlook..... 107

E-Mail-Untersuchung in The Bat! 107

MAIL-ANTI-VIRUS AKTIVIEREN UND DEAKTIVIEREN

Mail-Anti-Virus ist standardmäßig aktiviert und arbeitet im optimalen Modus. Bei Bedarf kann Mail-Anti-Virus deaktiviert werden.

Gehen Sie folgendermaßen vor, um Mail-Anti-Virus zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Mail-Anti-Virus aktivieren**.

SCHUTZBEREICH FESTLEGEN

Unter Schutzbereich wird der Typ der Nachrichten verstanden, die untersucht werden sollen. Standardmäßig untersucht Kaspersky Internet Security sowohl eingehende, als auch ausgehende E-Mails.

Wenn Sie nur die Untersuchung eingehender E-Mails gewählt haben, ist es empfehlenswert, zu Beginn der Arbeit mit Kaspersky Internet Security die ausgehenden E-Mails zu untersuchen, weil sich auf Ihrem Computer Mailwürmer befinden können, die E-Mails als Kanal verwenden, um sich weiterzuverbreiten. Dadurch wird erlaubt, Probleme zu verhindern, die mit dem unkontrollierten Versenden infizierter E-Mails von Ihrem Computer verbunden sind.

Zum Schutzbereich gehören auch die Parameter für die Integration von Mail-Anti-Virus in das System und die zu untersuchenden Protokolle. In der Grundeinstellung wird Mail-Anti-Virus in die Mailprogramme Microsoft Office Outlook und The Bat! integriert.

Gehen Sie folgendermaßen vor, um die Untersuchung ausgehender E-Mails auszuschalten:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Schutzbereich** die Variante **Nur eingehende Nachrichten**.

Gehen Sie folgendermaßen vor, um die zu untersuchenden Protokolle und die Parameter für die Integration von Mail-Anti-Virus in das System festzulegen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Integration ins System** die erforderlichen Parameter.

SICHERHEITSSTUFE ÄNDERN UND WIEDERHERSTELLEN

Abhängig von den aktuellen Erfordernissen können Sie eine vordefinierte Sicherheitsstufe für E-Mails wählen oder die Einstellungen von Mail-Anti-Virus entsprechend anpassen.

Die Spezialisten von Kaspersky Lab warnen davor, die Funktionsparameter von Mail-Anti-Virus zu verändern. In den meisten Fällen ist es ausreichend, eine andere Sicherheitsstufe zuwählen.

Während der Konfiguration von Mail-Anti-Virus können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese Einstellungen gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und entsprechen der Sicherheitsstufe **Empfohlen**.

Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe für E-Mails zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Stellen Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe ein oder klicken Sie auf **Einstellungen**, um die Untersuchungseinstellungen manuell anzupassen.

Wenn manuelle Änderungen erfolgen, ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Gehen Sie folgendermaßen vor, um die standardmäßigen Einstellungen für den Mail-Schutz wiederherzustellen,

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Standard**.

HEURISTISCHE ANALYSE VERWENDEN

Bei der Arbeit von Mail-Anti-Virus wird immer die Methode *Signaturanalyse* verwendet, bei der Kaspersky Internet Security ein gefundenes Objekt mit den Einträgen in den Datenbanken vergleicht.

Um die Effektivität des Schutzes zu steigern, können Sie eine *heuristische Analyse* verwenden (Analyse der Aktivität, die ein Objekt im System zeigt). Diese Analyse erlaubt die Erkennung neuer Schadobjekte, über die noch keine Datenbankeinträge vorliegen.

Gehen Sie folgendermaßen vor, um die Verwendung der heuristischen Analyse zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster **Allgemein** im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse** und stellen Sie darunter die Genauigkeitsstufe der Untersuchung ein.

AKTION FÜR GEFUNDENE OBJEKTE ÄNDERN

Beim Fund infizierter oder möglicherweise infizierter Objekte führt das Programm eine festgelegte Aktion aus.

Gehen Sie folgendermaßen vor, um die festgelegte Aktion für gefundene Objekte zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Wählen Sie auf der rechten Fensterseite im Block **Aktion beim Fund einer Bedrohung** die entsprechende Option aus.

ANLAGENFILTERUNG

Schädliche Programme werden am häufigsten als Anhänge einer Nachricht verbreitet. Um den Computer beispielsweise davor zu schützen, dass angehängte Dateien automatisch gestartet werden, können Sie die Anlagenfilterung aktivieren. Sie erlaubt es, Dateien bestimmter Typen automatisch umzubenennen oder zu löschen.

Gehen Sie folgendermaßen vor, um die Anlagenfilterung zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Anlagenfilterung** einen Filtermodus. Bei Auswahl der letzten beiden Modi wird die Liste der Dateitypen (Erweiterungen) aktiviert. In dieser Liste können Sie die erforderlichen Typen wählen oder die Maske eines neuen Typs hinzufügen.

   Um der Liste die Maske eines neuen Typs hinzuzufügen, klicken Sie auf den Link **Hinzufügen** und öffnen Sie das Fenster **Maske für einen Dateinamen**. Geben Sie dort die erforderlichen Daten ein.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie Archive, Datenbanken usw. Um Viren zu erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

Sie können die Untersuchung angehängter Archive aktivieren oder deaktivieren, sowie die maximale Größe der zu untersuchenden Archive begrenzen.

Wenn Ihr Computer nicht durch die Mittel eines lokalen Netzwerks geschützt ist (die Internetverbindung erfolgt ohne Proxyserver oder Firewall), wird davor gewarnt, die Untersuchung angehängter Archive zu deaktivieren.

Gehen Sie folgendermaßen vor, um die Untersuchungsparameter für zusammengesetzte Dateien anzupassen:

1. Öffnee das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Geben Sie im folgenden Fenster auf der Registerkarte **Allgemein** die entsprechenden Parameter an.

E-MAIL-UNTERSUCHUNG IN MICROSOFT OFFICE OUTLOOK

Wenn Microsoft Office Outlook als Mailprogramm verwendet wird, können Sie die Einstellungen für die Virenuntersuchung Ihrer E-Mails zusätzlich anpassen.

Bei der Installation von Kaspersky Internet Security wird ein spezielles Erweiterungsmodul in Microsoft Office Outlook integriert. Es erlaubt Ihnen, schnell zu den Einstellungen von Mail-Anti-Virus zu wechseln und festzulegen, wann eine E-Mail-Nachricht auf das Vorhandensein gefährlicher Objekte untersucht werden soll.

Das Erweiterungsmodul besitzt die Form einer Registerkarte mit dem Namen **E-Mail-Schutz**, die sich im Menü **Extras** → **Optionen** befindet.

Gehen Sie folgendermaßen vor, um zu wählen, wann die Untersuchung von E-Mails erfolgen soll:

1. Öffnen Sie das Hauptfenster von Microsoft Office Outlook.
2. Wählen Sie im Programmmenü den Punkt **Extras** → **Optionen**.
3. Wählen Sie auf der Registerkarte **E-Mail-Schutz** die erforderlichen Parameter.

E-MAIL-UNTERSUCHUNG IN THE BAT!

Die Aktionen für infizierte E-Mail-Objekte werden im Mailprogramm The Bat! durch Mittel des Programms festgelegt.

Die Parameter von Mail-Anti-Virus, die festlegen, ob ein- und ausgehende E-Mails untersucht werden oder nicht, und die Aktionen für gefährliche E-Mail-Objekte und Ausnahmen bestimmen, werden ignoriert. Das Programm The Bat! berücksichtigt lediglich die Untersuchung angehängter Archive.

Die Parameter für den E-Mail-Schutz gelten für alle auf dem Computer installierten Antiviren-Komponenten, die die Arbeit mit The Bat! unterstützen.

Es sollte beachtet werden, dass E-Mails beim Empfang zuerst von Mail-Anti-Virus untersucht werden und erst anschließend von dem Plug-in des Mailprogramms The Bat!. Wenn ein schädliches Objekt gefunden wird, werden Sie von Kaspersky Internet Security auf jeden Fall darüber informiert. Wenn dabei im Meldungsfenster von Mail-Anti-Virus die Aktion **Desinfizieren** (**Löschen**) gewählt wird, führt Mail-Anti-Virus das Löschen der Bedrohung aus. Wird im Meldungsfenster die Aktion **Überspringen** gewählt, so wird das Objekt von dem Plug-in für The Bat! desinfiziert. Beim Senden werden E-Mails zuerst von dem Plug-in und anschließend von Mail-Anti-Virus untersucht.

Legen Sie folgende Kriterien fest:

- Welche Richtung des E-Mail-Verkehrs (eingehend, ausgehend) der Virenuntersuchung unterzogen werden soll.
- Wann die Untersuchung von Mail-Objekten erfolgen soll (beim Öffnen einer Mail oder vor dem Speichern auf der Festplatte).
- Welche Aktionen das Mailprogramm ausführen soll, wenn gefährliche Objekte gefunden werden. Es stehen beispielsweise zur Auswahl:
  - **Reparaturversuch infizierter Teile** – Bei Auswahl dieser Variante wird versucht, ein infiziertes Objekt zu desinfizieren. Wenn die Desinfektion fehlschlägt, verbleibt das Objekt in der Nachricht.
  - **Infizierte Teile löschen** – Bei Auswahl dieser Variante wird ein gefährliches E-Mail-Objekt gelöscht. Dabei bleibt unberücksichtigt, ob es infiziert ist oder als verdächtig gilt.

Standardmäßig verschiebt das Programm The Bat! alle infizierten E-Mail-Objekte ohne Desinfektion in die Quarantäne.

E-Mail-Nachrichten, die gefährliche Objekte enthalten, werden von dem Programm The Bat! nicht durch eine spezielle Kopfzeile gekennzeichnet.

Gehen Sie folgendermaßen vor, um in The Bat! die Einstellungen für den E-Mail-Schutz anzupassen:

1. Öffnen Sie das Hauptfenster von The Bat!.
2. Wählen Sie im Menü **Optionen** des Mailprogramms den Punkt **Benutzereinstellungen**.
3. Wählen Sie in der Konfigurationsstruktur das Objekt **Virenschutz**.

WEB-ANTI-VIRUS

Bei der Arbeit im Internet besteht für die Informationen, die auf Ihrem Computer gespeichert sind, ständig das Risiko einer Infektion durch gefährliche Programme. Sie können in Ihren Computer eindringen, während Sie kostenlose Programme herunterladen oder scheinbar ungefährliche Webseiten besuchen (die zuvor von Hackern angegriffen wurden). Außerdem können Netzwürmer direkt beim Aufbau einer Internetverbindung in Ihren Computer eindringen, noch bevor eine Webseite geöffnet oder eine Datei heruntergeladen wurde.

Die Sicherheit Ihrer Arbeit im Internet wird von der Komponente *Web-Anti-Virus* gewährleistet. Er schützt Informationen, die über die Protokolle HTTP, HTTPS und FTP auf Ihren Computer gelangen, und verhindert auf Ihrem Computer den Start gefährlicher Skripts.

Der Web-Schutz sieht nur die Kontrolle des Datenstroms vor, der über die Ports übertragen wird, die auf der Liste der kontrollierten Ports stehen. Eine Liste der Ports, die am häufigsten zur Datenübertragung dienen, ist im Lieferumfang von Kaspersky Internet Security enthalten. Wenn Sie Ports verwenden, die nicht zu dieser Liste gehören, fügen Sie diese zur Liste der kontrollierten Ports hinzu (s. Abschnitt "Liste der zu kontrollierenden Ports erstellen" auf S. 142), um den Schutz des über sie abgewickelten Datenverkehrs sicherzustellen.

Die Untersuchung des Datenstroms erfolgt mit einer bestimmten Auswahl von Parametern, die als Sicherheitsstufe bezeichnet wird (s. Abschnitt "Sicherheitsstufe für Web-Anti-Virus wählen" auf S. 111). Beim Fund von Bedrohungen führt Web-Anti-Virus die festgelegte Aktion aus.

Die Spezialisten von Kaspersky Lab warnen davor, die Funktionsparameter von Web-Anti-Virus zu verändern. In den meisten Fällen ist es ausreichend, eine passende Sicherheitsstufe zu wählen.

Algorithmus für die Arbeit der Komponente

Web-Anti-Virus schützt Informationen, die über das HTTP-, HTTPS- und FTP-Protokoll auf Ihren Computer gelangen oder von ihm gesendet werden, und verhindert auf Ihrem Computer den Start gefährlicher Skripts. Die Untersuchung geschützter Verbindungen (nach HTTPS-Protokoll) ist standardmäßig deaktiviert. Sie kann aktiviert und angepasst werden (s. Abschnitt "Untersuchung geschützter Verbindungen" auf S. 139).

Der Schutz der Daten erfolgt nach folgendem Algorithmus:

1. Jede Webseite oder Datei, auf die ein Benutzer oder ein bestimmtes Programm über die Protokolle HTTP, HTTPS oder FTP zugreift, wird von Web-Anti-Virus abgefangen und auf schädlichen Code analysiert. Die Suche nach schädlichen Objekten erfolgt auf Basis der Datenbanken, die bei der Arbeit von Kaspersky Internet Security verwendet werden, sowie mit Hilfe eines heuristischen Algorithmus. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten schädlichen Programme und entsprechende Desinfektionsmethoden. Der heuristische Algorithmus erlaubt es, neue Viren zu erkennen, die noch nicht in den Datenbanken beschrieben sind.

2. Aufgrund der Virenuntersuchung bestehen folgende Varianten für das weitere Vorgehen:

   - Wenn eine Webseite oder ein Objekt, auf das ein Benutzer zugreift, schädlichen Code enthält, wird der Zugriff darauf blockiert. Dabei erscheint auf dem Bildschirm eine Meldung darüber, dass das angeforderte Objekt oder die Seite infiziert ist.

   - Wenn die Datei oder Webseite keinen schädlichen Code enthält, erhält der Benutzer sofort Zugriff darauf.

Die Untersuchung von Skripts wird nach folgendem Algorithmus ausgeführt:

1. Jedes auszuführende Skript wird von Web-Anti-Virus abgefangen und auf schädlichen Code analysiert.

2. Wenn ein Skript schädlichen Code enthält, wird es von Web-Anti-Virus gesperrt und der Benutzer wird durch eine spezielle Bildschirmmeldung darüber informiert.

3. Wenn im Skript kein schädlicher Code gefunden wird, wird es ausgeführt.

Web-Anti-Virus fängt nur Skripts ab, die auf der Technologie Microsoft Windows Script Host basieren.

IN DIESEM ABSCHNITT

Web-Anti-Virus aktivieren und deaktivieren 110

Sicherheitsstufe für Web-Anti-Virus wählen 111

Aktionen für gefährliche Objekte wählen 111

Link-Untersuchung mit den Datenbanken für verdächtige und Phishing-Adressen 112

Heuristische Analyse verwenden 112

Gefährliche Skripts blockieren 113

Untersuchung optimieren 113

Modul zur Link-Untersuchung 114

Zugriff auf gefährliche Webseiten blockieren 115

Zugriff auf regionale Domains kontrollieren 115

Zugriff auf Online-Banking-Dienste kontrollieren 116

Liste mit vertrauenswürdigen Adressen erstellen 116

Einstellungen für Web-Anti-Virus wiederherstellen 116

WEB-ANTI-VIRUS AKTIVIEREN UND DEAKTIVIEREN

Die Komponente kann auf zwei Arten aktiviert und deaktiviert werden.

- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47)
- aus dem Konfigurationsfenster (s. Abschnitt "Programmkonfigurationsfenster" auf S. 52).

Gehen Sie folgendermaßen vor, um Web-Anti-Virus vom Hauptfenster aus zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Schutz-Center**.
2. Öffnen Sie auf der rechten Fensterseite durch Linksklick den Block **Kontrolle der Arbeit im Netzwerk** oder den Block **Schutz für System und Programme**.
3. Klicken Sie auf **Web-Anti-Virus**, um das Menü zur Auswahl einer Aktion für die Komponente zu öffnen, und gehen Sie dort auf **Web-Anti-Virus aktivieren**, um die Komponente zu aktivieren, oder auf Web-Anti-Virus deaktivieren, um die Komponente zu deaktivieren.

   Wird eine Komponente aktiviert, so wird das Symbol links von ihrem Namen grün, wird sie deaktiviert, so wird das Symbol grau.

Gehen Sie folgendermaßen vor, um Web-Anti-Virus vom Hauptfenster aus zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Web-Anti-Virus** aktivieren, um die Komponente einzuschalten. Deaktivieren Sie das Kontrollkästchen, um Anti-Banner auszuschalten.

SICHERHEITSSTUFE FÜR WEB-ANTI-VIRUS WÄHLEN

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Parametern für Web-Anti-Virus verstanden, die eine bestimmte Schutzstufe für die Daten gewährleistet, die mit den Protokollen HTTP, HTTPS und FTP empfangen und gesendet werden. Die Kaspersky-Lab-Experten haben drei Sicherheitsstufen vordefiniert.

- hoch – Gewährleistet maximalen Schutz, der bei der Arbeit in einer gefährlichen Umgebung erforderlich ist.
- empfohlen – Gewährleistet optimalen Schutz und wird für die meisten Fälle empfohlen.
- niedrig – Gewährleistet maximale Performance.

Sie treffen selbst eine Entscheidung über die Auswahl der Sicherheitsstufe, wobei Ihre Arbeitsbedingungen und die aktuelle Situation berücksichtigt werden sollten.

Gehen Sie folgendermaßen vor, um eine der vordefinierten Sicherheitsstufen zu wählen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Wählen Sie auf der rechten Fensterseite mit Hilfe des Schiebereglers die gewünschte Sicherheitsstufe.

Wenn keine der vordefinierten Stufen Ihren Anforderungen entspricht, können Sie die Einstellungen von Web-Anti-Virus anpassen. Sie können z.B. das Genauigkeitsniveau der Untersuchung für die heuristische Analyse ändern. Wenn die Einstellungen verändert werden, ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Wenn Sie zu einer der vordefinierten Sicherheitsstufen zurückkehren möchten, stellen Sie die Einstellungen der Komponente wieder her (s. Abschnitt "Einstellungen für Web-Anti-Virus wiederherstellen" auf S. 116).

AKTIONEN FÜR GEFÄHRLICHE OBJEKTE WÄHLEN

Wenn sich bei der Analyse eines Objekts im Web-Datenverkehr herausstellt, dass das Objekt schädlichen Code enthält, sind die weiteren Operationen von Web-Anti-Virus von der Aktion abhängig, die Sie festgelegt haben.

Was die Aktionen für gefährliche Skripts betrifft, so sperrt Web-Anti-Virus deren Ausführung immer und zeigt auf dem Bildschirm eine Meldung an, die den Benutzer über die ausgeführte Aktion informiert. Die Aktion für ein gefährliches Skript kann nicht geändert werden, es ist nur möglich, die Skript-Untersuchung zu deaktivieren (s. Abschnitt "Gefährliche Skripts blockieren" auf S. 113).

Wenn Sie im automatischen Modus arbeiten, wendet Kaspersky Internet Security beim Fund gefährlicher Objekte automatisch die von Kaspersky Lab empfohlene Aktion an.

Gehen Sie folgendermaßen vor, um eine Aktion für gefundene Objekte zu wählen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Wählen Sie auf der rechten Fensterseite im Block **Aktion beim Fund einer Bedrohung** die Variante, die das Programm auf ein gefundenes gefährliches Objekt anwenden soll.

LINK-UNTERSUCHUNG MIT DEN DATENBANKEN FÜR VERDÄCHTIGE UND PHISHING-ADRESSEN

Web-Anti-Virus kann den Web-Datenverkehr auf Viren untersuchen und feststellen, ob Links auf der Liste für verdächtige Webadressen oder auf der Liste für Phishing-Webadressen stehen.

Durch die Untersuchung von Links auf die Zugehörigkeit zur Liste der Phishing-Adressen lassen sich Phishing-Angriffe abwehren, die in der Regel die Form von E-Mails besitzen, die scheinbar von finanziellen Strukturen stammen und Links auf deren Webseiten enthalten. Die Nachricht fordert dazu auf, einem Link zu folgen und auf der betreffenden Webseite vertrauliche Informationen wie beispielsweise eine Kreditkartennummer oder Benutzername und Kennwort für die persönliche Online-Banking-Seite einzugeben, auf der finanzielle Operationen erfolgen können. Ein häufiges Beispiel für Phishing-Angriffe ist ein Brief, der scheinbar von einer Bank stammt, bei der Sie Kunde sind, und einen Link zu der offiziellen Webseite der Bank enthält. Wenn Sie dem Link folgen, gelangen Sie auf eine Webseite, die eine genaue Kopie der Bankseite darstellt und im Browser sogar deren Adresse anzeigen kann, obwohl Sie sich in Wirklichkeit auf einer fiktiven Webseite befinden. Alle Aktionen, die Sie auf dieser Webseite ausführen, werden verfolgt und können zum Diebstahl Ihres Geldes missbraucht werden.

Listen mit Phishing-Webadressen gehören zum Lieferumfang von Kaspersky Internet Security. Da sich ein Phishing-Link nicht nur in E-Mails, sondern beispielsweise auch im Text einer ICQ-Nachricht befinden kann, überwacht Web-Anti-Virus alle Versuche zum Öffnen einer Phishing-Seite auf der Ebene des Web-Datenverkehrs und blockiert den Zugriff auf solche Webseiten.

Gehen Sie folgendermaßen vor, damit Web-Anti-Virus alle Links mit den Datenbanken für verdächtige und Phishing-Webadressen untersucht:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.
4. Vergewissern Sie sich, dass auf der Registerkarte **Allgemein** im Block **Untersuchungsmethoden** die Kontrollkästchen **Links mit der Datenbank für verdächtige Webadressen untersuchen** und **Links mit der Datenbank für Phishing-Webadressen untersuchen** aktiviert sind.

HEURISTISCHE ANALYSE VERWENDEN

Die *heuristische Analyse* ist eine spezielle Untersuchungsmethode. Mit ihrer Hilfe wird die Aktivität analysiert, die ein Objekt im System zeigt. Wenn diese Aktivität als typisch für schädliche Objekte gilt, lässt sich das Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen, selbst wenn der enthaltene Schadcode den Virenanalytikern noch unbekannt ist.

Sie können eine Genauigkeitsstufe der Untersuchung für die heuristischen Analyse festlegen:

- oberflächlich – schnelle Untersuchung
- tief – detaillierte Untersuchung, die am meisten Zeit beansprucht.
- mittel – optimale Kombination aus Geschwindigkeit und Untersuchungsgenauigkeit, die für die meisten Fälle passend ist.

Wenn aufgrund der heuristischen Analyse ein schädliches Objekt gefunden wird, werden Sie von Kaspersky Internet Security darüber informiert und Sie können wählen, welche Aktion auf das gefundene Objekt anzuwenden ist.

Die heuristische Analyse ist standardmäßig aktiviert und die Untersuchung erfolgt mit der Genauigkeitsstufe **mittel**.

Gehen Sie folgendermaßen vor, um die heuristische Analyse zu aktivieren und eine Genauigkeitsstufe für die Untersuchung zu wählen, oder um die heuristische Analyse zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.
4. Um die heuristische Analyse zu aktivieren, aktivieren Sie auf der Registerkarte **Allgemein** im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse**. Legen Sie unten mit Hilfe des Schiebereglers die Genauigkeitsstufe der Untersuchung fest. Deaktivieren Sie das Kontrollkästchen **Heuristische Analyse**, wenn diese Untersuchungsmethode nicht verwendet werden soll.

GEFÄHRLICHE SKRIPTS BLOCKIEREN

Web-Anti-Virus kann alle Skripts, die in Microsoft Internet Explorer verarbeitet werden, und alle WSH-Skripts (JavaScript, Visual Basic Script u.a.), die bei der Arbeit eines Benutzers auf dem Computer gestartet werden, untersuchen. Wenn ein Skript den Computer gefährden kann, wird seine Ausführung blockiert.

Gehen Sie folgendermaßen vor, damit Web-Anti-Virus Skripts untersucht und blockiert:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.
4. Vergewissern Sie sich, dass auf der Registerkarte **Allgemein** im Block **Erweitert** das Kontrollkästchen **Gefährliche Skripts in Microsoft Internet Explorer blockieren aktiviert ist**.

UNTERSUCHUNG OPTIMIEREN

Um die Effektivität der Erkennung von schädlichem Code durch Web-Anti-Virus zu steigern, wird für Objekte, die aus dem Internet eintreffen, die Zwischenspeicherung von Fragmenten verwendet. Bei Verwendung dieser Methode wird ein Objekt erst von Web-Anti-Virus untersucht, nachdem es vollständig empfangen wurde. Anschließend wird das Objekt auf Viren analysiert und entsprechend der Analyseergebnisse dem Benutzer zur Arbeit übergeben oder blockiert.

Die Zwischenspeicherung erhöht die Verarbeitungs- und Bereitstellungsdauer für ein Objekt. Außerdem kann es durch die Zwischenspeicherung zu Problemen beim Laden und bei der Verarbeitung großer Objekte kommen, die mit einer Zeitüberschreitung für die Verbindung zum HTTP-Client zusammenhängen.

Um dieses Problem zu lösen, empfehlen wir, eine Dauer für die Zwischenspeicherung von Fragmenten für ein Objekt festzulegen. Bei einer Überschreitung der festgelegten Dauer wird jeder heruntergeladene Teil des Objekts ungeprüft an den Benutzer übergeben. Nach Abschluss des Downloads wird das Objekt vollständig gescannt. Dadurch lässt sich die Bereitstellungsdauer des Objekts an den Benutzer verkürzen und das Problem einer Verbindungstrennung lösen. Gleichzeitig bleibt das Sicherheitsniveau bei der Arbeit im Internet aufrechterhalten.

Wird die Zeitbeschränkung für die Zwischenspeicherung aufgehoben, so erhöht sich die Effektivität der Antiviren-Untersuchung, wobei es aber gleichzeitig zu einer gewissen Verzögerung beim Objektzugriff kommt.

Gehen Sie folgendermaßen vor, um die Zeit für die Zwischenspeicherung von Fragmenten zu beschränken oder diese Beschränkung aufzuheben:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.

4. Um die Dauer der Zwischenspeicherung des Datenverkehrs zu beschränken, aktivieren Sie auf der Registerkarte **Allgemein** im Block **Erweitert** das Kontrollkästchen **Cachedauer für den Datenverkehr beschränken, um die Untersuchung zu optimieren**. Wenn keine Beschränkung erforderlich ist, deaktivieren Sie das Kontrollkästchen.

MODUL ZUR LINK-UNTERSUCHUNG

Kaspersky Internet Security umfasst ein Modul zur Link-Untersuchung, das zu der Komponente Web-Anti-Virus gehört. Das Modul wird als Plug-in in die Webbrowser Microsoft Internet Explorer und Mozilla Firefox integriert.

Das Modul untersucht alle Links, die auf einer Webseite vorhanden sind, auf Zugehörigkeit zu verdächtigen und Phishing-Webadressen. Sie können folgende Listen anlegen: eine Liste mit Webseiten, deren Inhalt nicht auf verdächtige und Phishing-Links untersucht werden soll, oder eine Liste mit Webseiten, deren Inhalt untersucht werden soll. Sie können die Link-Untersuchung auch ganz ausschalten.

Die unten genannten Konfigurationsvarianten für das Modul zur Link-Untersuchung können nicht nur im Programmkonfigurationsfenster, sondern auch im Konfigurationsfenster des Moduls ausgeführt werden. Letzteres wird vom Webbrowser aus geöffnet.

- *Gehen Sie folgendermaßen vor, um eine Liste der Webadressen anzulegen, deren Inhalt nicht auf verdächtige und Phishing-Links untersucht werden soll:*

  1. Öffnen Sie das Programmkonfigurationsfenster.

  2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

  3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

     Das Fenster **Web-Anti-Virus** wird geöffnet.

  4. Wählen Sie auf der Registerkarte **Web-Filter** im Block **Modul zur Link-Untersuchung** die Variante **In allen Webadressen, außer bei Ausnahmen** und klicken Sie auf **Ausnahmen**.

  5. Legen Sie im folgenden Fenster **Ausnahmen** eine Liste der Webadressen an, deren Inhalt nicht auf verdächtige und Phishing-Links untersucht werden soll.

- *Gehen Sie folgendermaßen vor, um eine Liste der Webadressen anzulegen, deren Inhalt auf verdächtige und Phishing-Links untersucht werden soll:*

  1. Öffnen Sie das Programmkonfigurationsfenster.

  2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

  3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

     Das Fenster **Web-Anti-Virus** wird geöffnet.

  4. Wählen Sie auf der Registerkarte **Web-Filter** im Block **Modul zur Link-Untersuchung** die Variante **Nur in den festgelegten Webadressen** und klicken Sie auf **Festlegen**.

  5. Legen Sie im folgenden Fenster **Zu untersuchende Webadressen** eine Liste der Webadressen an, deren Inhalt auf verdächtige und Phishing-Links untersucht werden soll.

- *Gehen Sie folgendermaßen vor, damit das Modul keine Links untersucht:*

  1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.

4. Deaktivieren Sie auf der Registerkarte **Web-Filter** im Block **Modul zur Link-Untersuchung** das Kontrollkästchen **Links untersuchen**.

Um das Konfigurationsfenster für die Link-Untersuchung aus dem Webbrowser zu öffnen,

klicken Sie in der Symbolleiste des Browsers auf die Schaltfläche mit dem Symbol von Kaspersky Internet Security.

ZUGRIFF AUF GEFÄHRLICHE WEBSEITEN BLOCKIEREN

Sie können den Zugriff auf Webseiten blockieren, die vom Modul zur Link-Untersuchung als verdächtig oder als Phishing-Seiten eingestuft wurden (s. Abschnitt "Modul zur Link-Untersuchung" auf S. 114).

Wenn das Programm nicht eindeutig feststellen kann, ob eine Webseite, auf die ein Link verweist, gefährlich ist, besteht die Möglichkeit, sie im Modus "Sicherer Browser" zu laden (s. S. 168) (nur bei der Arbeit in den Webbrowsern Microsoft Internet Explorer und Mozilla Firefox). Bei der Arbeit in der Sicheren Umgebung stellen schädliche Objekte keine Gefahr für Ihren Computer dar.

Gehen Sie folgendermaßen vor, um den Zugriff auf gefährliche Webseiten zu blockieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Web-Filter** im Block **Modul zum Blockieren gefährlicher Webseiten** das Kontrollkästchen **Gefährliche Webseiten blockieren**.

ZUGRIFF AUF REGIONALE DOMAINS KONTROLLIEREN

Bei aktiviertem Geo-Filter kann Web-Anti-Virus nach Vorgabe des Benutzers den Zugriff auf Webseiten je nach ihrer Zugehörigkeit zu regionalen Internet-Domains verbieten oder erlauben. Dadurch lässt sich beispielsweise der Zugriff auf Webseiten verbieten, die regionalen Domains mit einem hohem Kontaminationsgrad angehören.

Gehen Sie folgendermaßen vor, um den Zugriff auf Webseiten, die bestimmten regionalen Domains angehören, zu erlauben oder zu verbieten:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

4. Das Fenster **Web-Anti-Virus** wird geöffnet.

5. Aktivieren Sie auf der Registerkarte **Geo-Filter** das Kontrollkästchen **Filterung nach regionalen Domains aktivieren** und geben Sie darunter in der Liste der kontrollierten Domains an, auf welche Domains der Zugriff erlaubt oder verboten werden soll, und für welche Domains das Programm mit Hilfe einer Meldung um Zugriffserlaubnis fragen soll (s. Abschnitt "Erlaubnisanfrage für den Zugriff auf eine Webseite aus einer regionalen Domain" auf S. 216).

Für regionale Domains, die Ihrem Standort entsprechen, ist der Zugriff standardmäßig erlaubt. Für alle übrigen Domains ist standardmäßig eine Anfrage auf Zugriffserlaubnis vorgesehen.

ZUGRIFF AUF ONLINE-BANKING-DIENSTE KONTROLLIEREN

Beim Online-Banking benötigt der Benutzer einen besonderen Schutz, da ein Verlust sensibler Daten in diesem Fall zu finanziellen Nachteilen führen kann. Web-Anti-Virus kann den Zugriff aufs Internet-Banking kontrollieren und dessen sichere Nutzung gewährleisten (s. Abschnitt "Sicherer Browser" auf S. 168). Web-Anti-Virus ermittelt automatisch, welche Internetressourcen zu Online-Banking-Diensten gehören. Damit eine Internetressource garantiert als Online-Banking-Dienst identifiziert wird, können Sie ihre Adresse einer entsprechenden Liste hinzufügen.

Gehen Sie folgendermaßen vor, um die Kontrolle für den Zugriff auf Online-Banking-Dienste zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Online-Banking** das Kontrollkästchen **Kontrolle aktivieren**. Nun wird Ihnen vorgeschlagen, den Assistenten zur Zertifikatsinstallation zu starten, mit dem Sie das Kaspersky-Lab-Zertifikat für die Untersuchung von geschützten Verbindungen installieren können.
5. Erstellen Sie bei Bedarf eine Liste der Ressourcen, die das Programm obligatorisch als Online-Banking-Dienste identifizieren soll.

LISTE MIT VERTRAUENSWÜRDIGEN ADRESSEN ERSTELLEN

Sie können eine Liste der Webadressen anlegen, deren Inhalt Sie vorbehaltlos vertrauen. Web-Anti-Virus wird die Informationen von diesen Adressen nicht auf gefährliche Objekte hin analysieren. Diese Option kann beispielsweise verwendet werden, wenn Web-Anti-Virus den Download einer bestimmten Datei von einer Ihnen bekannten Webseite verhindert.

Gehen Sie folgendermaßen vor, um eine Liste mit vertrauenswürdigen Adressen anzulegen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Vertrauenswürdige Adressen** das Kontrollkästchen **Web-Datenverkehr von vertrauenswürdigen Webadressen nicht untersuchen** und legen Sie eine Liste der Webadressen an, deren Inhalt Sie vertrauen.

Um eine Adresse vorübergehend aus der vertrauenswürdigen Liste auszuschließen, ohne sie aus der Liste zu löschen, deaktivieren Sie das entsprechende Kontrollkästchen .

EINSTELLUNGEN FÜR WEB-ANTI-VIRUS WIEDERHERSTELLEN

Um Einstellungsänderungen für Web-Anti-Virus rückgängig zu machen, können Sie die von Kaspersky Lab empfohlenen Einstellungen wiederherstellen. Diese Einstellungen entsprechen der Sicherheitsstufe **Empfohlen**.

Gehen Sie folgendermaßen vor, um die standardmäßigen Einstellungen für Web-Anti-Virus wiederherzustellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Standard**.

   Die Sicherheitsstufe erhält den Wert **Empfohlen**.

IM-ANTI-VIRUS

IM-Anti-Virus untersucht den Datenverkehr, der mit Programmen zum Sofortaustausch von Nachrichten (so genannte *Instant Messenger*) übertragen wird.

Nachrichten, die mit Instant Messengern übertragen werden, können Links zu Webseiten enthalten, die verdächtig sind oder die von Angreifern für Phishing-Angriffe verwendet werden. Schädliche Programme verwenden Instant Messenger zum Senden von Spam-Nachrichten. Außerdem können Sofortnachrichten Links zu Programmen (oder sogar Programme) enthalten, die Nummern und Kennwörter von Benutzern stehlen.

Kaspersky Internet Security gewährleistet Sicherheit bei der Arbeit mit einer Vielzahl von Programmen, die dem Sofortaustausch von Nachrichten dienen. Dazu zählen ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent und IRC.

Manche Instant Messenger wie z.B. Yahoo! Messenger und Google Talk verwenden eine geschützte Verbindung. Um den Datenverkehr dieser Programme zu untersuchen, muss die Untersuchung von geschützten Verbindungen aktiviert werden (s. S. 139).

Die Nachrichten werden von IM-Anti-Virus abgefangen und auf gefährliche Objekte und Links geprüft. Sie können die Nachrichtentypen (s. S. 118) wählen, die untersucht werden sollen, und unterschiedliche Untersuchungsmethoden einsetzen.

Wenn IM-Anti-Virus in einer Nachricht eine Bedrohung findet, wird die Nachricht durch eine Warnung für den Benutzer ersetzt.

Dateien, die über einen Instant Messenger übertragen werden, werden von der Komponente Datei-Anti-Virus untersucht, wenn versucht wird sie zu speichern.

IN DIESEM ABSCHNITT

IM-Anti-Virus aktivieren und deaktivieren 117

Schutzbereich festlegen 118

Untersuchungsmethode wählen 118

IM-ANTI-VIRUS AKTIVIEREN UND DEAKTIVIEREN

IM-Anti-Virus ist standardmäßig aktiviert und arbeitet im optimalen Modus. Bei Bedarf kann IM-Anti-Virus deaktiviert werden.

Gehen Sie folgendermaßen vor, um IM-Anti-Virus zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **IM-Anti-Virus**.

3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **IM-Anti-Virus aktivieren**.

SCHUTZBEREICH FESTLEGEN

Unter Schutzbereich wird der Typ der Nachrichten verstanden, die untersucht werden sollen. Standardmäßig untersucht Kaspersky Internet Security sowohl eingehende, als auch ausgehende E-Mails. Wenn Sie sicher sind, dass die von Ihnen gesendeten Nachrichten keine gefährlichen Objekte enthalten, können Sie die Untersuchung des ausgehenden Datenverkehrs deaktivieren.

- *Gehen Sie folgendermaßen vor, um die Untersuchung ausgehender Nachrichten zu deaktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **IM-Anti-Virus**.

3. Wählen Sie auf der rechten Fensterseite im Block **Schutzbereich** die Variante **Nur eingehende Nachrichten**.

UNTERSUCHUNGSMETHODE AUSWÄHLEN

Die Untersuchungsmethoden beziehen sich hier auf die Untersuchung der in Instant Messenger-Nachrichten enthaltenen Links auf ihre Zugehörigkeit zur Liste für verdächtige Adressen und (oder) zur Liste der Phishing-Adressen.

Um die Effektivität des Schutzes zu steigern, können Sie eine *heuristische Analyse* verwenden (Analyse der Aktivität, die ein Objekt im System zeigt). Diese Analyse erlaubt die Erkennung neuer Schadobjekte, über die noch keine Datenbankeinträge vorliegen. Bei der heuristischen Analyse werden alle Skripts, die in Instant Messenger-Nachrichten enthalten sind, in der einer geschützten Umgebung ausgeführt. Wenn die erkannte Aktivität eines Skripts als typisch für schädliche Objekte gilt, lässt sich das Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen. In der Grundeinstellung ist die heuristische Analyse aktiviert.

- *Gehen Sie folgendermaßen vor, um die in E-Mails enthaltenen Links mit der Datenbank für verdächtige Adressen zu untersuchen:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **IM-Anti-Virus**.

3. Aktivieren Sie auf der rechten Fensterseite im Block **Untersuchungsmethoden** das Kontrollkästchen **Links mit der Datenbank für verdächtige Webadressen untersuchen**.

- *Gehen Sie folgendermaßen vor, um die in E-Mails enthaltenen Links mit der Datenbank für Phishing-Adressen zu untersuchen:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **IM-Anti-Virus**.

3. Aktivieren Sie auf der rechten Fensterseite im Block **Untersuchungsmethoden** das Kontrollkästchen **Links mit der Datenbank für Phishing-Webadressen untersuchen**.

- *Gehen Sie folgendermaßen vor, um die Verwendung der heuristischen Analyse zu aktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **IM-Anti-Virus**.

3. Aktivieren Sie auf der rechten Fensterseite im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse** und stellen Sie darunter das Genauigkeitsniveau ein.

PROAKTIVER SCHUTZ

Der Proaktive Schutz bietet Schutz vor neuen Bedrohungen, über die in den Datenbanken von Kaspersky Internet Security keine Informationen vorhanden sind.

Die präventiven Technologien, auf denen der Proaktive Schutz beruht, erlauben es, einen Zeitverlust zu vermeiden und eine neue Bedrohung zu neutralisieren, bevor sie auf Ihrem Computer Schaden verursachen kann. Im Unterschied zu den reaktiven Technologien, bei denen die Analyse auf Basis von Einträgen der Datenbanken von Kaspersky Internet Security erfolgt, identifizieren die Präventivtechnologien eine neue Bedrohung auf Ihrem Computer nach den Aktionsfolgen, die von einem bestimmten Programm ausgeführt werden. Wenn aufgrund der Aktivitätsanalyse die Aktionsfolge eines Programms als verdächtig eingestuft wird, sperrt Kaspersky Internet Security seine Aktivität.

Werden beispielsweise Aktionen erkannt, bei denen sich ein bestimmtes Programm selbst in eine Netzwerkressource, in den Autostart-Ordner und in die Systemregistrierung kopiert, so handelt es sich mit hoher Wahrscheinlichkeit um einen Wurm. Als gefährliche Aktionsfolgen gelten auch Änderungsversuche der HOSTS-Datei, versteckte Treiberinstallation u.a. Sie können für eine bestimmte gefährliche Aktivität die Kontrolle deaktivieren (s. S. 120) oder die entsprechenden Kontrollregeln ändern (S. S. 120).

Im Unterschied zur Programmkontrolle reagiert der Proaktive Schutz genau auf bestimmte Aktionsfolgen eines Programms. Die Aktivitätsanalyse erstreckt sich auf alle Programme, einschließlich der Programme, die von der Komponente Programmkontrolle der Gruppe **Vertrauenswürdig** zugeordnet wurden.

Sie können für den proaktiven Schutz eine Gruppe mit vertrauenswürdigen Programmen anlegen (s. S. 120). Über die Aktivität solcher Programme werden keine Meldungen angezeigt.

Wenn ein Computer mit den Betriebssystemen Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 oder Microsoft Windows 7 x64 arbeitet, werden nicht alle Ereignisse kontrolliert. Dies hängt mit Besonderheiten der genannten Betriebssysteme zusammen. Nicht in vollem Umfang kontrolliert werden beispielsweise das Senden von Daten über vertrauenswürdige Programme und verdächtige Aktivität im System.

IN DIESEM ABSCHNITT

Proaktiven Schutz aktivieren und deaktivieren 119

Gruppe mit vertrauenswürdigen Programmen erstellen 120

Liste der gefährlichen Aktivität verwenden 120

Kontrollregel für gefährliche Aktivität ändern 120

PROAKTIVEN SCHUTZ AKTIVIEREN UND DEAKTIVIEREN

Der Proaktive Schutz ist standardmäßig aktiviert und arbeitet im optimalen Modus. Sie können den Proaktiven Schutz bei Bedarf deaktivieren.

Gehen Sie folgendermaßen vor, um den Proaktiven Schutz zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** die Komponente **Proaktiver Schutz**.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **Proaktiven Schutz aktivieren**.

GRUPPE MIT VERTRAUENSWÜRDIGEN PROGRAMMEN ERSTELLEN

Programme, die von der Komponente Programmkontrolle den Status **Vertrauenswürdig** erhalten, stellen keine Gefahr für das System dar. Trotzdem wird ihre Aktivität von der Komponente Proaktiver Schutz kontrolliert. Sie können eine Gruppe mit vertrauenswürdigen Programmen erstellen, deren Aktivität nicht vom Proaktiven Schutz überwacht werden soll. Als vertrauenswürdig gelten standardmäßig jene Programme, die eine verifizierte digitale Signatur besitzen oder in der Datenbank von Kaspersky Security Network enthalten sind.

Gehen Sie folgendermaßen vor, um die Einstellungen zu ändern, die für das Anlegen einer Gruppe für vertrauenswürdige Programme gelten:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** die Komponente **Proaktiver Schutz**.
3. Aktivieren Sie auf der rechten Fensterseite im Block **Vertrauenswürdige Programme** die Kontrollkästchen für die entsprechenden Parameter.

LISTE DER GEFÄHRLICHEN AKTIVITÄT VERWENDEN

Die Liste der Aktionen, die als gefährliche Aktivität gelten, kann nicht verändert werden. Dabei können Sie die Kontrolle bestimmter Typen gefährlicher Aktivität deaktivieren.

Gehen Sie folgendermaßen vor, um die Kontrolle bestimmter Typen gefährlicher Aktivität zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** die Komponente **Proaktiver Schutz**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Deaktivieren Sie im folgenden Fenster **Proaktiver Schutz** das Kontrollkästchen neben dem Namen des Aktivitätstyps, der nicht kontrolliert werden soll.

KONTROLLREGEL FÜR GEFÄHRLICHE AKTIVITÄT ÄNDERN

Aktionen für Programme, deren Aktivität als gefährlich klassifiziert wurde, können nicht geändert werden. Sie können folgende Aktionen ausführen:

- die Kontrolle bestimmter Typen gefährlicher Aktivität deaktivieren (s. S. 120).
- Liste von Ausnahmen (s. S. 181) erstellen, indem Sie die Programme festlegen, deren Aktivität Sie nicht für gefährlich halten.
- Regel ändern, nach welcher der Proaktive Schutz beim Fund einer gefährlichen Aktivität vorgeht.

Gehen Sie folgendermaßen vor, um eine Regel für den Proaktiven Schutz zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** die Komponente **Proaktiver Schutz**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster **Proaktiver Schutz** in der Spalte **Ereignis** das Ereignis, für das die Regel geändert werden soll.
5. Legen Sie für das gewählte Ereignis mit Hilfe der Links im Block **Regelbeschreibung** die entsprechenden Parameter fest: Beispielsweise:

a. Klicken Sie auf den Link mit der geltenden Aktion und wählen Sie im folgenden Fenster **Aktion wählen** die entsprechende Aktion.

b. Klicken Sie auf den Link **Ein / Aus**, um festzulegen, ob die ausgeführte Operation protokolliert werden soll.

AKTIVITÄTSMONITOR

Der Aktivitätsmonitor sammelt Daten über die Aktionen der Programme auf Ihrem Computer und versorgt die anderen Schutzkomponenten mit entsprechenden Informationen, um die Effektivität des Schutzes zu steigern.

Wenn die Speicherung eines Aktivitätsverlaufs der Programme aktiviert ist, kann der Aktivitätsmonitor ein Rollback von Malware-Aktionen (s. S. 122) ausführen. Wenn eine schädliche Aktivität erkannt wird, kann ein Rollback von Aktionen auf folgende Weise initiiert werden: von der Komponente Aktivitätsmonitor auf Basis von Vorlagen für gefährliches Verhalten (s. Abschnitt "Vorlagen für gefährliches Verhalten verwenden (BSS)" auf S. 122), vom Proaktiven Schutz sowie bei der Ausführung einer Untersuchungsaufgabe oder bei der Arbeit von Datei-Anti-Virus (s. S. 97).

Wenn die Aktionen von Programmen mit den Vorlagen für gefährliches Verhalten übereinstimmen, ist die Reaktion der Komponente vom Funktionsmodus für Kaspersky Internet Security abhängig.

Werden im System verdächtige Ereignisse gefunden, so können die Schutzkomponenten von Kaspersky Internet Security zusätzliche Informationen vom Aktivitätsmonitor anfordern. Sofern Kaspersky Internet Security im interaktiven Modus arbeitet, stehen die Daten über einen Vorfall, die von der Komponente Aktivitätsmonitor gesammelt wurden, als Bericht über den Verlauf gefährlicher Aktivitäten zur Verfügung. Dadurch bietet sich eine Entscheidungshilfe, wenn im Meldungsfenster eine Aktion gewählt werden muss. Wenn die Komponente ein potentiell gefährliches Programm findet, erscheint im Meldungsfenster (s. S. 217) mit der Aktionsanfrage oben ein Link, der zu einem Bericht des Aktivitätsmonitors führt.

IN DIESEM ABSCHNITT

Aktivitätsmonitor aktivieren und deaktivieren 121

Vorlagen für gefährliches Verhalten verwenden (BSS) 122

Rollback von Aktionen eines schädlichen Programms 122

AKTIVITÄTSMONITOR AKTIVIEREN UND DEAKTIVIEREN

Der Aktivitätsmonitor ist standardmäßig aktiviert und richtet seine Arbeit nach dem Modus, der für Kaspersky Internet Security eingestellt wurde (automatisch oder interaktiv).

Es wird davor gewarnt, die Komponente auszuschalten, wenn es nicht unbedingt erforderlich ist, weil dadurch die Effektivität des Proaktiven Schutzes eingeschränkt wird. Außerdem können auch andere Schutzkomponenten beeinträchtigt werden, die von Daten abhängig sind, die der Aktivitätsmonitor sammelt, um gefundene potentielle Bedrohungen besser zu beurteilen.

➧ *Gehen Sie folgendermaßen vor, um die Aktivitätsmonitor zu deaktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Aktivitätsmonitor**.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Aktivitätsmonitor aktivieren**.

VORLAGEN FÜR GEFÄHRLICHES VERHALTEN VERWENDEN (BSS)

Vorlagen für gefährliches Programmverhalten (BSS – Behavior Stream Signatures) enthalten Aktionsfolgen für Programme, die als gefährlich klassifiziert wurden. Wenn die Aktivität eines Programms mit einer Aktivität aus den Vorlagen für gefährliches Verhalten übereinstimmt, führt Kaspersky Internet Security eine vorgegebene Aktion aus.

Die Verhaltensvorlagen, die der Aktivitätsmonitor verwendet, werden im Rahmen des Updates von Kaspersky Internet Security laufend ergänzt, um einen aktuellen und effektiven Schutz zu garantieren.

Wenn Kaspersky Internet Security im automatischen Modus arbeitet, verschiebt der Aktivitätsmonitor das betreffende Programm standardmäßig in die Quarantäne, wenn die Programmaktivität mit einer Vorlage für gefährliches Verhalten übereinstimmt. Im interaktiven Modus (s. S. 83) wird der Benutzer nach einer Aktion gefragt. Sie können eine Aktion festlegen, die ausgeführt werden soll, wenn die Aktivität eines Programms mit einer Vorlage für gefährliches Verhalten übereinstimmt.

Neben einer präzisen Übereinstimmung der Programmaktivität mit einer Vorlage für gefährliches Verhalten erkennt der Aktivitätsmonitor auch Aktionen, die partiell mit Vorlagen für gefährliches Verhalten identisch sind und aufgrund einer heuristischen Analyse als verdächtig gelten. Beim Fund einer verdächtigen Aktivität fragt der Aktivitätsmonitor den Benutzer unabhängig vom Funktionsmodus nach einer Aktion.

- *Gehen Sie folgendermaßen vor, um die Aktion für eine Übereinstimmung von Programmaktivität und Vorlage für gefährliches Verhalten zu wählen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Aktivitätsmonitor**.
3. Aktivieren Sie auf der rechten Fensterseite im Block **Heuristische Analyse** das Kontrollkästchen **Aktualisierbare Vorlagen für gefährliches Verhalten verwenden**.
4. Wählen Sie die Option **Aktion ausführen** aus und dann, in der Dropdown-Liste, die gewünschte Aktion.

ROLLBACK VON AKTIONEN EINES SCHÄDLICHEN PROGRAMMS

Sie können eine Option verwenden, mit der die Aktionen schädlicher Programm im System rückgängig gemacht werden können. Für das Rollback muss der Aktivitätsmonitor den Verlauf der Programmaktivität speichern.

Standardmäßig erfolgt bei der Arbeit mit Kaspersky Internet Security im Automatikmodus bei Erkennung einer schädlichen Aktivität durch die Schutzkomponenten ein automatisches Rollback. Im interaktiven Modus (s. S. 83) fragt der Aktivitätsmonitor den Benutzer nach der auszuführenden Aktion. Sie können eine Aktion angeben, die bei Erkennung einer schädlichen Aktivität ausgeführt werden soll.

Das Rollback der Aktionen schädlicher Programme betrifft lediglich ganz bestimmte Daten. Es hat keinerlei negativen Einfluss auf die Funktion des Betriebssystems und führt nicht zu Datenverlust auf Ihrem Computer.

- *Gehen Sie folgendermaßen vor, um ein Rollback von Aktionen, die von einem schädlichen Programm ausgeführt wurden, anzupassen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Aktivitätsmonitor**.
3. Aktivieren Sie auf der rechten Fensterseite im Block **Verlauf der Programmaktivität** das Kontrollkästchen **Verlauf der Programmaktivität speichern**.
4. Wählen Sie die Option **Aktion ausführen** aus und dann, in der Dropdown-Liste, die gewünschte Aktion.

PROGRAMMKONTROLLE

Die Programmkontrolle hindert Programme daran, systemgefährliche Aktionen auszuführen, und kontrolliert den Zugriff auf Betriebssystemressourcen und auf Ihre persönlichen Daten.

Die Komponente verfolgt die Aktionen, die von auf dem Computer installierten Programmen im System ausgeführt werden, und reguliert ihre Aktivität entsprechend den Regeln der Programmkontrolle. Diese Regeln regulieren eine potentiell gefährliche Aktivität. Dazu zählt der Zugriff der Programme auf geschützte Ressourcen (Dateien und Ordner, Registrierungsschlüssel, Netzwerkadressen usw.).

Die Netzwerkaktivität von Programmen wird von der KomponenteFirewall kontrolliert (s. S. 132).

Wenn ein Programm zum ersten Mal auf dem Computer gestartet wird, untersucht die Komponente Programmkontrolle seine Sicherheit und verschiebt das Programm in eine der Sicherheitsgruppen. Die Sicherheitsgruppe bestimmt die Regeln, die Kaspersky Internet Security zur Aktivitätskontrolle dieses Programms verwenden wird. Die Regeln der Programmkontrolle bestehen aus einer Auswahl von Rechten für den Zugriff auf Computerressourcen und von Beschränkungen für unterschiedliche Programmaktionen auf dem Computer.

Sie können die Bedingungen für die Zuordnung von Programmen zu den einzelnen Gruppen anpassen (s. S. 124), ein Programm in eine andere Gruppe verschieben (s. S. 125), und die Regeln für Kaspersky Internet Security ändern (s. S. 126).

Es wird empfohlen, am Kaspersky Security Network teilzunehmen, um die Optimierung der Programmkontrolle zu unterstützen. Die Daten, die mit Hilfe des Kaspersky Security Network ermittelt werden, erlauben es, Programme genauer zu einer bestimmten Sicherheitsgruppe zuzuordnen und optimale Regeln zur Programmkontrolle zu verwenden .

Beim wiederholten Start eines Programms kontrolliert die Programmkontrolle seine Integrität. Wenn ein Programm nicht verändert wurde, wendet die Komponente die aktuellen Regeln darauf an. Wenn ein Programm verändert wurde, überprüft die Programmkontrolle es erneut wie beim ersten Start.

Um den Zugriff von Programmen auf unterschiedliche Ressourcen des Computers zu kontrollieren, können Sie die vorgegebene Liste für geschützte Ressourcen verwenden oder die Liste durch benutzerdefinierte Ressourcen erweitern (s. S. 130).

IN DIESEM ABSCHNITT

Programmkontrolle aktivieren und deaktivieren 123

Programme zu Sicherheitsgruppen zuordnen 124

Aktivität von Programmen anzeigen 125

Sicherheitsgruppe ändern und Standardgruppe wiederherstellen 125

Arbeit mit den Regeln der Programmkontrolle 126

Schutz für Betriebssystemressourcen und persönliche Daten 130

Interpretation von Daten über die Verwendung eines Programms durch die KSN-Teilnehmer 131

PROGRAMMKONTROLLE AKTIVIEREN UND DEAKTIVIEREN

Standardmäßig ist die Programmkontrolle aktiviert und arbeitet in einem von Kaspersky Lab entwickelten Modus, Sie können sie jedoch bei Bedarf deaktivieren.

Gehen Sie folgendermaßen vor, um die Programmkontrolle zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Schutz-Center**.
2. Öffnen Sie auf der rechten Seite durch Linksklick die Komponentenliste **Schutz für System und Programme**.
3. Wählen Sie die Komponente **Programmkontrolle**.
4. Wählen Sie im Kontextmenü den Punkt **Programmkontrolle deaktivieren**.

PROGRAMME ZU SICHERHEITSGRUPPEN ZUORDNEN

Wenn ein Programm zum ersten Mal auf dem Computer gestartet wird, untersucht die Komponente Programmkontrolle seine Sicherheit und verschiebt das Programm in eine der Sicherheitsgruppen.

Auf der ersten Etappe zur Überprüfung eines Programms durchsucht Kaspersky Internet Security eine interne Datenbank für bekannte Programme nach einem Eintrag über das Programm und schickt anschließend eine Anfrage an die Datenbank des Kaspersky Security Network (s. Abschnitt "Teilnahme am Kaspersky Security Network" auf S. 201) (sofern eine Internetverbindung besteht). Wenn in der Datenbank ein Eintrag zum Programm gefunden wird, wird das Programm in die Gruppe verschoben, die in der Datenbank angegeben ist.

Programme, die keine Gefahr für das System darstellen, werden in die Gruppe **Vertrauenswürdig** verschoben. In diese Gruppe werden standardmäßig solche Programme verschoben, die eine digitale Signatur besitzen oder deren übergeordnetes Objekt eine digitale Signatur besitzt. Sie können das automatische Verschieben von Programmen mit einer digitalen Signatur in die Gruppe **Vertrauenswürdig** deaktivieren.

Das Verhalten von Programmen, die von der Programmkontrolle in die Gruppe **Vertrauenswürdig** verschoben werden, wird trotzdem von der Komponente Proaktiver Schutz kontrolliert (auf S. 119)

Um die entsprechenden Gruppen für unbekannte Programme zu ermitteln (Programme, die nicht in der Datenbank von Kaspersky Security Network enthalten sind und keine digitale Signatur besitzen), verwendet Kaspersky Internet Security standardmäßig eine heuristische Analyse. Bei dieser Analyse erfolgt eine Risikobewertung des Programms, auf deren Basis das Programm in eine bestimmte Gruppe verschoben wird. Anstelle einer heuristischen Analyse können Sie eine Gruppe festlegen, in die Kaspersky Internet Security alle unbekannten Programme automatisch verschieben soll.

Die Programmkontrolle untersucht ein Programm standardmäßig im Verlauf von 30 Sekunden. Wenn die Risikobewertung innerhalb dieses Zeitraums nicht abgeschlossen wurde, wird das Programm in die Gruppe **Schwach beschränkt** verschoben und die Risikobewertung wird im Hintergrundmodus fortgesetzt. Anschließend wird das Programm endgültig in eine Gruppe verschoben. Sie können die Dauer ändern, für die gestartete Programme untersucht werden sollen. Wenn Sie sicher sind, dass alle Programme, die auf Ihrem Computer gestartet werden, sicher sind, können Sie die für die Untersuchung vorgesehene Dauer verringern. Sollten Sie riskante Software auf dem Computer installieren, so wird empfohlen, die Untersuchungsdauer zu erhöhen.

Wenn sich ein hoher Risikowert ergibt, werden Sie von Kaspersky Internet Security darüber informiert und Sie können eine Gruppe wählen, der das Programm zugeordnet werden soll. Die Meldung (s. S. 215) enthält eine Statistik über die Verwendung dieses Programms durch die Teilnehmer von Kaspersky Security Network. Diese Statistik und ein Verlauf über die Aktivitäten des Programms auf Ihrem Computer unterstützen Sie bei einer möglichst objektiven Entscheidung darüber, in welche Gruppe das Programm verschoben werden soll (s. Abschnitt "Interpretation von Daten über die Verwendung eines Programms durch die KSN-Teilnehmer" auf S. 131).

*Gehen Sie folgendermaßen vor, damit Programme mit einer digitalen Signatur nicht automatisch in die Gruppe **Vertrauenswürdig** verschoben werden:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Deaktivieren Sie auf der rechten Fensterseite **Begrenzungen festlegen** das Kontrollkästchen **Programmen mit digitaler Signatur vertrauen**.

- *Gehen Sie folgendermaßen vor, um die heuristische Analyse zur Ermittlung der Gruppen für unbekannte Programme zu verwenden:*

  1. Öffnen Sie das Programmkonfigurationsfenster.
  2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
  3. Wählen Sie im rechten Fensterbereich im Block **Begrenzungen festlegen** die Variante **Zur Ermittlung einer Gruppe die heuristische Analyse verwenden**.

- *Gehen Sie folgendermaßen vor, um die Dauer für Ermittlung einer Gruppe zu ändern:*

  1. Öffnen Sie das Programmkonfigurationsfenster.
  2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
  3. Ändern Sie im rechten Fensterbereich im Block **Begrenzungen festlegen** den Parameterwert **Maximale Dauer für die Ermittlung einer Programmgruppe**.

- *Gehen Sie folgendermaßen vor, damit alle unbekannten Programme in eine festgelegte Gruppe verschoben werden:*

  1. Öffnen Sie das Programmkonfigurationsfenster.
  2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
  3. Wählen Sie im rechten Fensterbereich im Block **Begrenzungen festlegen** die Variante **Automatisch verschieben in die Gruppe** und wählen Sie die entsprechende Gruppe aus der Dropdown-Liste.

AKTIVITÄT VON PROGRAMMEN ANZEIGEN

Angezeigt werden können Informationen über alle Programme, die auf Ihrem Computer verwendet werden, und über alle Prozesse, die momentan ausgeführt werden.

- *Gehen Sie folgendermaßen vor, um eine Übersicht über die Programmaktivität anzuzeigen:*

  1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Schutz-Center** aus.
  2. Öffnen Sie auf der rechten Fensterseite durch Linksklick die Komponentenliste **Schutz für System und Programme**.
  3. Klicken Sie auf den Link **Programmaktivität**.
  4. Wählen Sie im folgenden Fenster **Programmaktivität** links oben in der Dropdown-Liste eine entsprechende Programmkategorie.

SICHERHEITSGRUPPE ÄNDERN UND STANDARDGRUPPE WIEDERHERSTELLEN

Wenn ein Programm zum ersten Mal gestartet wird, verschiebt Kaspersky Internet Security das Programm automatisch in die entsprechende Gruppe (s. Abschnitt "Programme zu Sicherheitsgruppen zuordnen" auf S. 124). Falls erforderlich, können Sie ein Programm manuell in eine andere Gruppe verschieben. Sie können ein Programm jederzeit wieder der standardmäßig vorgegebenen Gruppe zuweisen..

Die Kaspersky-Lab-Experten warnen davor, Programme aus den Gruppen, denen sie automatisch zugewiesen wurden, in andere Gruppen zu verschieben. Ändern Sie stattdessen bei Bedarf die Regeln für ein bestimmtes Programm (s. Abschnitt "Programmregeln ändern" auf S. 127).

Gehen Sie folgendermaßen vor, um ein Programm in eine andere Gruppe zu verschieben:

1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Schutz-Center**.
2. Öffnen Sie auf der rechten Fensterseite durch Linksklick die Komponentenliste **Schutz für System und Programme**.
3. Klicken Sie auf den Link **Programmaktivität**.
4. Wählen Sie im folgenden Fenster **Programmaktivität** links oben in der Dropdown-Liste eine entsprechende Programmkategorie.
5. Öffnen Sie durch Rechtsklick das Kontextmenü für das betreffende Programm und wählen Sie dort den Punkt **Verschieben in Gruppe → <Name der Gruppe>**.

Gehen Sie folgendermaßen vor, um einem Programm wieder den automatisch zugewiesenen Status zuzuweisen:

1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Schutz-Center**.
2. Öffnen Sie auf der rechten Fensterseite durch Linksklick die Komponentenliste **Schutz für System und Programme**.
3. Klicken Sie auf den Link **Programmaktivität**.
4. Wählen Sie im folgenden Fenster **Programmaktivität** links oben in der Dropdown-Liste eine entsprechende Programmkategorie.
5. Öffnen Sie durch Rechtsklick das Kontextmenü für das betreffende Programm und wählen Sie den Punkt **Standardgruppe wiederherstellen → <Name der Gruppe>**.

ARBEIT MIT DEN REGELN DER PROGRAMMKONTROLLE

Die Regeln der Programmkontrolle bestehen aus einer Auswahl von Rechten für den Zugriff auf Computerressourcen und von Beschränkungen für unterschiedliche Programmaktionen auf dem Computer.

In der Grundeinstellung werden für die Programmkontrolle die Regeln jener Sicherheitsgruppe verwendet, in die ein Programm bei seinem ersten Start von Kaspersky Internet Security verschoben wurde. Die Gruppenregeln wurden von Kaspersky-Lab-Experten erarbeitet, um eine optimale Kontrolle der Programmaktivität zu gewährleisten. Bei Bedarf können Sie diese Regeln ändern oder sie für ein bestimmtes Programm anpassen. Regeln für ein Programm besitzen eine höhere Priorität als Regeln für eine Gruppe.

IN DIESEM ABSCHNITT

Gruppenregeln ändern 126

Programmregeln ändern 127

Herunterladen von Regeln aus dem Kaspersky Security Network 128

Vererbung von Beschränkungen eines übergeordneten Prozesses 129

Regeln für nicht verwendete Programme löschen 129

GRUPPENREGELN ÄNDERN

In der Grundeinstellung sind für die einzelnen Sicherheitsgruppen optimale Rechte für den Zugriff auf Computerressourcen vorgegeben. Sie können die vordefinierten Gruppenregeln ändern.

Gehen Sie folgendermaßen vor, um Gruppenregeln zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie auf der rechten Fensterseite im Block **Rechte für Programme und geschützte Ressourcen anpassen** auf **Programme**.
4. Wählen Sie im folgenden Fenster **Programme** die betreffende Gruppe aus der Liste und klicken Sie auf **Ändern**.
5. Wählen Sie im folgenden Fenster **Gruppenregeln** die Registerkarte, die der betreffenden Ressourcenkategorie entspricht (**Dateien und Systemregistrierung**, **Rechte**).
6. Öffnen Sie durch Rechtsklick in der Spalte der entsprechenden Aktion das Kontextmenü für die entsprechende Ressource und wählen Sie dort den entsprechenden Wert (**Erlauben**, **Verbieten** oder **Aktion erfragen**).

PROGRAMMREGELN ÄNDERN

Sie können die Begrenzungen für ein einzelnes Programm ändern oder mehrere Aktionen aus Programmregeln ausschließen. Kaspersky Internet Security kontrolliert die Aktionen nicht, die als Ausnahmen für Programmregeln hinzugefügt wurden.

Alle Ausnahmen, die in den Regeln für Programme erstellt wurden, stehen im Konfigurationsfenster für die Programmparameter (s. Abschnitt"Programmkonfigurationsfenster" auf S. 52) im Abschnitt **Gefahren und Ausnahmen** zur Verfügung.

Außerdem können Sie die Verwendung von Gruppenregeln für die Zugriffskontrolle auf bestimmte Kategorien der geschützten Ressourcen deaktivieren. Der Zugriff des Programms auf diese Ressourcen wird dann durch die Regeln für das Programm gesteuert.

Gehen Sie folgendermaßen vor, um eine Regel für ein Programm zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie auf der rechten Fensterseite im Block **Rechte für Programme und geschützte Ressourcen anpassen** auf **Programme**.
4. Wählen Sie im folgenden Fenster **Programme** das betreffende Programm aus der Liste und klicken Sie auf **Ändern**.
5. Öffnen Sie im folgenden Fenster **Programmregeln** die Registerkarte, die der erforderlichen Ressourcenkategorie entspricht (**Dateien und Systemregistrierung,**, **Rechte**).
6. Öffnen Sie durch Rechtsklick in der Spalte der entsprechenden Aktion das Kontextmenü für die entsprechende Ressource und wählen Sie dort den entsprechenden Wert (**Erlauben**, **Verbieten** oder **Aktion erfragen**).

Gehen Sie folgendermaßen vor, um die Vererbung von Gruppenregeln für den Zugriff auf Ressourcen zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie auf der rechten Fensterseite im Block **Rechte für Programme und geschützte Ressourcen anpassen** auf **Programme**.
4. Wählen Sie im folgenden Fenster **Programme** das erforderliche Programm aus der Dropdown-Liste aus.

5. Klicken Sie auf **Ändern**.

6. Öffnen Sie im folgenden Fenster **Programmregeln** die Registerkarte, die der erforderlichen Ressourcenkategorie entspricht (**Dateien und Systemregistrierung,**, **Rechte**).

7. Öffnen Sie durch Rechtsklick in der Spalte der entsprechenden Aktion das Kontextmenü für die entsprechende Ressource und wählen Sie dort den Punkt **Erben**, für den das Kontrollkästchen aktiviert ist.

Gehen Sie folgendermaßen vor, um eine Ausnahme zu Programmregeln hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.

3. Klicken Sie auf der rechten Fensterseite im Block **Rechte für Programme und geschützte Ressourcen anpassen** auf **Programme**.

4. Wählen Sie im folgenden Fenster **Programme** das betreffende Programm aus der Liste und klicken Sie auf **Ändern**.

5. Wählen Sie im folgenden Fenster **Programmregeln** die Registerkarte **Ausnahmen.**

6. Aktivieren Sie die Kontrollkästchen für die Aktionen, die nicht kontrolliert werden sollen.

HERUNTERLADEN VON REGELN AUS DEM KASPERSKY SECURITY NETWORK

Für Programme, die in der Datenbank von Kaspersky Security Network gefunden wurden, werden standardmäßig die aus dieser Datenbank geladenen Regeln verwendet.

Wenn ein Programm beim ersten Start nicht in der Datenbank von Kaspersky Security Network verzeichnet war, danach jedoch entsprechende Programminformationen hinzugefügt wurden, werden die Regeln für die Kontrolle dieses Programms automatisch von Kaspersky Internet Security aktualisiert.

Sie können das Herunterladen der Regeln aus dem Kaspersky Security Network und (oder) die automatische Aktualisierung der Regeln für bisher unbekannte Programme deaktivieren.

Gehen Sie folgendermaßen vor, um das Herunterladen von Regeln aus dem Kaspersky Security Network zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.

3. Deaktivieren Sie auf der rechten Fensterseite im Block **Begrenzungen festlegen** das Kontrollkästchen **Regeln für Programme aus dem Kaspersky Security Network (KSN) herunterladen**.

Um die Aktualisierung der Regeln aus dem Kaspersky Security Network für bisher unbekannte Programme zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.

3. Deaktivieren Sie auf der rechten Fensterseite im Block **Begrenzungen festlegen** das Kontrollkästchen **Regeln für bisher unbekannte Programme aus KSN aktualisieren**.

VERERBUNG VON BESCHRÄNKUNGEN EINES ÜBERGEORDNETEN PROZESSES

Als Initiator für den Start eines Programms kann entweder der Benutzer oder ein anderes laufendes Programm auftreten. Wenn ein anderes Programm als Initiator auftritt, entsteht eine Startfolge, die übergeordnete und untergeordnete Programme umfasst.

Wenn ein Programm versucht, Zugriff auf eine geschützte Ressource zu erhalten, analysiert die Programmkontrolle für alle übergeordneten Programmprozesse die Zugriffsrechte auf die Ressource. Dabei wird die Regel mit der minimalen Priorität ausgeführt: Beim Vergleich von Zugriffsrechten eines Programms und eines übergeordneten Prozesses werden auf die Programmaktivität die Zugriffsrechte mit der geringsten Priorität angewendet.

Priorität der Zugriffsrechte:

1. Erlauben. Diese Zugriffsrechte besitzen die höchste Priorität.
2. Aktion erfragen.
3. Verbieten. Diese Zugriffsrechte besitzen die niedrigste Priorität.

Dieser Mechanismus verhindert, dass vertrauenswürdige Programme von zweifelhaften Programmen oder von Programmen, die über beschränkte Rechte verfügen, dazu benutzt werden, privilegierte Aktionen auszuführen.

Wenn die Aktivität eines Programms blockiert wird, weil ein übergeordneter Prozess unzureichende Rechte besitzt, können Sie diese Rechte anpassen (s. Abschnitt "Programmregeln ändern" auf S. 127).

Das Ändern von Rechten eines übergeordneten Prozesses oder das Ausschalten des Vererbungsmechanismus sollte nur dann erfolgen, wenn Sie absolut sicher sind, dass die Aktivität des Prozesses keine Gefahr für das System darstellt!

Gehen Sie folgendermaßen vor, um die Vererbung von Beschränkungen eines übergeordneten Prozesses zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie auf der rechten Fensterseite im Block **Rechte für Programme und geschützte Ressourcen anpassen** auf **Programme**.
4. Wählen Sie im folgenden Fenster **Programme** das erforderliche Programm aus der Dropdown-Liste aus.
5. Klicken Sie auf **Ändern**.
6. Wählen Sie im folgenden Fenster **Programmregeln** die Registerkarte **Ausnahmen**.
7. Aktivieren Sie dann das Kontrollkästchen **Beschränkungen des übergeordneten Prozesses (Programms) nicht übernehmen**.

REGELN FÜR NICHT VERWENDETE PROGRAMME LÖSCHEN

Standardmäßig werden die Regeln für Programme, die innerhalb der letzten 60 Tage nicht gestartet wurden, automatisch gelöscht. Sie können die Speicherdauer der Regeln für nicht verwendete Programme ändern oder das automatische Löschen deaktivieren.

Gehen Sie folgendermaßen vor, um eine Speicherdauer für Programmregeln festzulegen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.

3. Aktivieren Sie auf der rechten Fensterseite im Block **Erweitert** das Kontrollkästchen **Regeln für Programme löschen, wenn nicht gestartet seit** und geben Sie die entsprechende Anzahl der Tage an.

Gehen Sie folgendermaßen vor, um das automatische Löschen der Regeln für nicht verwendete Programme zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Deaktivieren Sie im rechten Fensterbereich im Block **Erweitert** das Kontrollkästchen **Regeln für Programme löschen, wenn nicht gestartet seit**.

SCHUTZ FÜR BETRIEBSSYSTEMRESSOURCEN UND PERSÖNLICHE DATEN

Die Programmkontrolle verwaltet die Rechte von Programmen, die für das Ausführen von Aktionen mit diversen Ressourcenkategorien des Betriebssystems und der persönlichen Daten gelten.

Die Kaspersky-Lab-Experten haben Kategorien für geschützte Ressourcen vordefiniert. Diese Liste kann nicht verändert werden. Sie können dieser Liste aber benutzerdefinierte Kategorien und / oder einzelne Ressourcen hinzufügen, und die Kontrolle bestimmter Ressourcen deaktivieren.

Außerdem können Sie bestimmte Ressourcen zu den Ausnahmen hinzufügen. Der Zugriff auf solche Ressourcen wird nicht kontrolliert.

Gehen Sie folgendermaßen vor, um geschützte persönliche Daten hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie auf der rechten Fensterseite auf **Ressourcen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Persönliche Daten** in der Dropdown-Liste die entsprechende Kategorie für persönliche Daten und öffnen Sie mit der Schaltfläche **Hinzufügen** das Fenster, in dem die Ressourcen hinzugefügt werden.
5. Legen Sie im folgenden Fenster **Benutzerressource** in Abhängigkeit von der hinzuzufügenden Ressource die notwendigen Parameter fest.

Nachdem eine Ressource hinzugefügt wurde, kann sie geändert oder gelöscht werden. Dazu dienen die entsprechenden Schaltflächen im oberen Bereich der Registerkarte. Um eine Ressource oder eine Kategorie von der Kontrolle auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

Gehen Sie folgendermaßen vor, um eine Kategorie für geschützte persönliche Daten zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie auf der rechten Fensterseite auf **Ressourcen**.
4. Öffnen Sie im folgenden Fenster auf der Registerkarte **Persönliche Daten** mit der Schaltfläche **Kategorie hinzufügen** das Fenster, in dem die Ressourcen hinzugefügt werden.
5. Geben Sie im folgenden Fenster **Kategorie für Benutzerressourcen** einen Namen für die neue Ressourcenkategorie ein.

Gehen Sie folgendermaßen vor, um geschützte Parameter und Ressourcen des Betriebssystems hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie auf der rechten Fensterseite auf **Ressourcen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Betriebssystem** in der Dropdown-Liste списке **Kategorie** die erforderliche Kategorie für Objekte des Betriebssystems aus.
5. Klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie im erscheinenden Menü den gewünschten Ressourcentyp aus.
6. Legen Sie im folgenden Fenster **Benutzerressource** in Abhängigkeit von der hinzuzufügenden Ressource die notwendigen Parameter fest.

Nachdem eine Ressource hinzugefügt wurde, kann sie geändert oder gelöscht werden. Dazu dienen die entsprechenden Schaltflächen im oberen Bereich der Registerkarte. Um eine Ressource oder eine Kategorie von der Kontrolle auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen.

Gehen Sie folgendermaßen vor, um den Ausnahmen eine Ressource hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie auf der rechten Fensterseite auf **Ressourcen**.
4. Betätigen Sie im erscheinenden Fenster auf der Registerkarte **Ausnahmen** die Schaltfläche **Hinzufügen** und wählen Sie im erscheinenden Menü den gewünschten Ressourcentyp.
5. Legen Sie im folgenden Fenster **Benutzerressource** in Abhängigkeit von der hinzuzufügenden Ressource die notwendigen Parameter fest.

INTERPRETATION VON DATEN ÜBER DIE VERWENDUNG EINES PROGRAMMS DURCH DIE KSN-TEILNEHMER

Die Informationen über die Verwendung eines Programms durch die Teilnehmer an Kaspersky Security Network (s. S. 201) können helfen, eine objektive Entscheidung darüber zu fällen, welcher Status einem Programm zugewiesen werden soll, das auf Ihrem Computer gestartet wird. Um die Gefährlichkeit eines Programms auf Grundlage der Daten aus dem KSN genau beurteilen zu können, sind genauere Informationen darüber erforderlich, wie das Programm auf Ihren Computer gekommen ist.

Die Kaspersky-Lab-Experten unterscheiden folgende möglichen Quellen für das Auftreten neuer Programme auf einem Computer.

- Download aus dem Internet und anschließender Start einer Installationsdatei durch den Benutzer
- Automatischer Download und Start einer Installationsdatei, wenn der Benutzer über einen Link auf eine Webseite wechselt.
- Der Benutzer startet eine Installationsdatei, die sich auf einer CD / DVD befindet oder von dort auf die Festplatte kopiert wurde.
- Der Benutzer startet eine Installationsdatei, die sich auf einem USB-Speicher befindet oder von dort auf die Festplatte kopiert wurde.
- Der Benutzer startet eine Installationsdatei, die per E-Mail, Instant Messenger oder über ein soziales Netzwerk empfangen wurde.

Die Statistik über die Verwendung eines Programms durch die Teilnehmer von Kaspersky Security Network enthält die Verwendungshäufigkeit und -dauer für das Programm. Für die Verwendung eines Programms bestehen folgende statistische Varianten:

- **sehr selten** (weniger als 100 KSN-Teilnehmer verwenden dieses Programm) und **kürzlich** (die Datei wurde vor einigen Tagen in KSN aufgenommen).
- **selten** (weniger als 1.000 KSN-Teilnehmer) und relativ **lange** (vor einigen Monaten). Die meisten Benutzer beschränken die Aktivität dieses Programms.
- **häufig** (über 100.000 KSN-Teilnehmer) und **lange** (vor über einem halben Jahr). Die meisten Benutzer vertrauen diesem Programm.
- **häufig** (über 100.000 KSN-Teilnehmer) und **kürzlich** (vor einigen Wochen). Die meisten Benutzer vertrauen diesem Programm oder beschränken es.
- **sehr häufig** (über 100.000 KSN-Teilnehmer) und **kürzlich**. Die meisten Benutzer vertrauen diesem Programm.

NETZWERKSCHUTZ

Unterschiedliche Schutzkomponenten, Tools und Konfigurationen von Kaspersky Internet Security bieten Ihnen Sicherheit bei der Arbeit in einem Netzwerk.

Die folgenden Abschnitte informieren ausführlich über folgende Themen: Funktionsprinzipien und Einstellungen der Firewall und des Schutzes vor Netzwerkangriffen, Netzwerkmonitor, Untersuchung von geschützten Verbindungen, Proxyserver-Einstellungen, Kontrolle von Netzwerkports.

IN DIESEM ABSCHNITT

Firewall 132

Schutz vor Netzwerkangriffen 137

Untersuchung geschützter Verbindungen 139

Netzwerkmonitor 141

Proxyserver-Einstellungen 142

Liste der zu kontrollierenden Ports erstellen 142

FIREWALL

Firewall gewährleistet Sicherheit bei der in lokalen Netzwerken und im Internet.

Die Komponente filtert die gesamte Netzwerkaktivität in Übereinstimmung mit den Netzwerkregeln der Programmkontrolle. Eine Netzwerkregel besteht aus einer Aktion, die von der Firewall ausgeführt wird, wenn ein Verbindungsversuch mit einem bestimmten Status erkannt wird. Jeder Netzwerkverbindung wird ein Status zugewiesen, der durch bestimmte Parameter definiert wird: Richtung und Protokoll für die Datenübertragung, Adressen und Ports, mit denen die Verbindung erfolgt.

Die Firewall analysiert die Parameter der Netzwerke, die Sie mit Ihrem Computer verbinden. Wenn das Programm im interaktiven Funktionsmodus arbeitet, fragt die Firewall Sie bei der ersten Verbindung nach dem Status des verbundenen Netzwerks (s. S. 215). Wenn der interaktive Funktionsmodus deaktiviert wurde, ermittelt die Firewall den Status, wozu Netzwerktyp, Adressenbereich und anderen Merkmale verwendet werden. Sie können den Status einer Netzwerkverbindung manuell ändern (s. S. 133).

IN DIESEM ABSCHNITT

Firewall aktivieren und deaktivieren 133

Netzwerkstatus ändern 133

Arbeit mit den Firewall-Regeln 133

Benachrichtigungen über Veränderungen eines Netzwerks anpassen 136

Erweiterte Einstellungen für die Firewall 136

FIREWALL AKTIVIEREN UND DEAKTIVIEREN

Firewall ist standardmäßig aktiviert und arbeitet im optimalen Modus. Bei Bedarf können Sie die Firewall deaktivieren.

Gehen Sie folgendermaßen vor, um die Firewall zu deaktivieren:

1. Öffnen Sie Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt Firewall.
2. Öffnen Sie auf der rechten Seite durch Linksklick die Komponentenliste **Schutz für System und Programme**.
3. Wählen Sie die Komponente **Firewall**.
4. Wählen Sie im Kontextmenü den Punkt **Firewall aktivieren**.

NETZWERKSTATUS ÄNDERN

Vom Status der Netzwerkverbindung hängt ab, welche Filterregeln für die Netzwerkaktivität dieser Verbindung zur Anwendung kommen. Bei Bedarf können Sie den Netzwerkstatus ändern.

Gehen Sie folgendermaßen vor, um den Status einer Netzwerkverbindung zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Netzwerke** eine aktive Netzwerkverbindung und klicken Sie auf **Ändern**, um das Konfigurationsfenster des Netzwerks zu öffnen.
5. Wählen Sie im folgenden Fenster auf der Registerkarte **Eigenschaften** den erforderlichen Status aus der Dropdown-Liste aus.

ARBEIT MIT DEN FIREWALL-REGELN

Die Firewall arbeitet mit zwei Arten von Regeln:

- *Paketregeln.* Dienen zur Definition von Beschränkungen für die Pakete, wobei das Programm keine Rolle spielt. Solche Regeln beziehen sich meistens auf die eingehende Netzwerkaktivität bestimmter Ports mit den Protokollen TCP und UDP und regulieren die Filterung von ICMP-Nachrichten.
- *Programmregeln*. Dienen zur Definition von Beschränkungen für die Netzwerkaktivität eines konkreten Programms. Solche Regeln erlauben es, die Aktivitätsfilterung genau anzupassen, wenn beispielsweise ein bestimmter Typ von Netzwerkverbindungen für konkrete Programme verboten, für andere aber erlaubt werden soll.

Paketregeln besitzen eine höhere Priorität als Programmregeln. Wenn für eine Art der Netzwerkaktivität gleichzeitig Paketregeln und Programmregeln vorhanden sind, wird diese Netzwerkaktivität nach den Paketregeln verarbeitet. Außerdem können Sie für jede Regel eine Ausführungspriorität (s. S. 135) festlegen.

PAKETREGEL ERSTELLEN

Paketregeln bestehen aus einer Kombination von Bedingungen und Aktionen, die unter bestimmten Bedingungen mit Paketen ausgeführt werden.

Wenn Sie Paketregeln erstellen, beachten Sie, dass diese eine höhere Priorität besitzen als Regeln für Programme.

Gehen Sie folgendermaßen vor, um eine neue Paketregel zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Paketregeln** auf die Schaltfläche **Hinzufügen**, um das Fenster für eine neue Netzwerkregel zu öffnen.
5. Legen Sie im folgenden Fenster **Netzwerkregel** die entsprechenden Parameter fest und klicken Sie auf **OK**.
6. Legen Sie die Priorität der neuen Regel fest, indem Sie sie mit Hilfe der Schaltflächen **Aufwärts** oder **Abwärts** in der Liste nach oben oder unten verschieben.

   Nachdem eine Regel erstellt wurde, können ihre Einstellungen geändert werden oder die Regel kann gelöscht werden. Dazu dienen die entsprechenden Schaltflächen im oberen Bereich der Registerkarte. Um eine Regel zu deaktivieren, entfernen Sie das Kontrollkästchen neben ihrem Namen.

GRUPPENREGELN ÄNDERN

Analog zur Komponente Programmkontrolle (s. S. 123) verwendet die Firewall zur Filterung der Netzwerkaktivität standardmäßig die Regeln der Gruppe, in die das Programm verschoben wurde.

Die Netzwerkregeln für die Sicherheitsgruppen legen fest, welche Rechte die Programme, die dieser Gruppe angehören, für den Zugriff auf unterschiedliche Netzwerke besitzen. Sie können die vordefinierten Netzwerkregeln einer Gruppe ändern oder neue Regeln hinzufügen.

Gehen Sie folgendermaßen vor, um eine Netzwerkregel für eine Gruppe hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Programmregeln** die betreffende Gruppe aus der Liste aus und klicken Sie auf **Ändern**.
5. Wählen Sie im folgenden Fenster **Gruppenregeln** die Registerkarte **Netzwerkregeln** und klicken Sie auf **Hinzufügen**.
6. Legen Sie im folgenden Fenster **Netzwerkregel** die entsprechenden Parameter fest und klicken Sie auf **OK**.
7. Legen Sie die Priorität der neuen Regel fest, indem Sie sie mit Hilfe der Schaltflächen **Aufwärts** oder **Abwärts** in der Liste nach oben oder unten verschieben.

   Nachdem eine Regel erstellt wurde, können ihre Einstellungen geändert werden oder die Regel kann gelöscht werden. Dazu dienen die entsprechenden Schaltflächen im oberen Bereich der Registerkarte. Um eine Regel zu deaktivieren, entfernen Sie das Kontrollkästchen neben ihrem Namen.

Gehen Sie folgendermaßen vor, um eine Netzwerkregel für eine Gruppe zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Programmregeln** die betreffende Gruppe aus der Liste aus und klicken Sie auf **Ändern**.
5. Wählen Sie im folgenden Fenster **Gruppenregeln** die Registerkarte **Netzwerkregeln**.
6. Öffnen Sie durch Rechtsklick in der Spalte **Erlaubnis** das Kontextmenü für die betreffende Regel und wählen Sie dort den entsprechenden Wert **(Erlauben**, **Verbieten** oder **Aktion erfragen**).

PROGRAMMREGELN ÄNDERN

Sie können Netzwerkregeln für bestimmte Programme erstellen. Netzwerkregeln für ein Programm besitzen eine höhere Priorität als Netzwerkregeln für eine Gruppe.

Bei Bedarf können Sie mit der Komponente Programmkontrolle Netzwerkregeln für Programme erstellen.

Gehen Sie folgendermaßen vor, um eine neue Netzwerkregel für ein Programm zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Programmregeln** ein Programm und klicken Sie auf **Ändern**, um das Konfigurationsfenster für Regeln zu öffnen.
5. Klicken Sie im folgenden Fenster auf der Registerkarte **Netzwerkregeln** auf die Schaltfläche **Hinzufügen**, um das Fenster für eine neue Netzwerkregel für das Programm zu öffnen.
6. Legen Sie im folgenden Fenster **Netzwerkregel** die entsprechenden Parameter fest und klicken Sie auf **OK**.
7. Legen Sie die Priorität der neuen Regel fest, indem Sie sie mit Hilfe der Schaltflächen **Aufwärts** oder **Abwärts** in der Liste nach oben oder unten verschieben.

   Nachdem eine Regel erstellt wurde, können ihre Einstellungen geändert werden oder die Regel kann gelöscht werden. Dazu dienen die entsprechenden Schaltflächen im oberen Bereich der Registerkarte. Um eine Regel zu deaktivieren, entfernen Sie das Kontrollkästchen neben ihrem Namen.

PRIORITÄT EINER REGEL ÄNDERN

Die Priorität für die Ausführung einer Regel wird durch ihre Position in der Liste bestimmt. Die erste Regel in der Liste besitzt die höchste Priorität.

Jede manuell neu erstellte Paketregel wird am Ende der Liste für Paketregeln hinzugefügt.

Die Gruppen für Programme sind nach Programmnamen angeordnet und die Priorität der Regeln gilt nur für eine bestimmte Gruppe. Benutzerdefinierte Regeln für Programme besitzen eine höhere Priorität als Regeln, die Gruppenregeln erben.

Gehen Sie folgendermaßen vor, um die Priorität einer Paketregel zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Paketregeln** eine Regel und verschieben Sie sie durch Klicken auf **Aufwärts** oder **Abwärts** an die erforderliche Position der Liste.

Gehen Sie folgendermaßen vor, um die Priorität von Regeln für ein Programm zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Programmregeln** ein Programm und klicken Sie auf **Ändern**, um das Konfigurationsfenster für Regeln zu öffnen.

5. Wählen Sie im folgenden Fenster auf der Registerkarte **Netzwerkregeln** eine Regel und verschieben Sie sie durch Klicken auf **Aufwärts** oder **Abwärts** an die erforderliche Position der Liste.

BENACHRICHTIGUNGEN ÜBER VERÄNDERUNGEN EINES NETZWERKS ANPASSEN

Die Parameter von Netzwerkverbindungen können sich im Verlauf der Arbeit ändern. Sie können sich über Einstellungsveränderungen informieren lassen:

Gehen Sie folgendermaßen vor, um die Benachrichtigungen über Veränderungen der Parameter einer Netzwerkverbindung anzupassen:

1. Öffnee das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Netzwerke** eine aktive Netzwerkverbindung und klicken Sie auf die Schaltfläche **Ändern**, um das Konfigurationsfenster des Netzwerks zu öffnen.

5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** die Kontrollkästchen für die Ereignisse, über die eine Meldung erfolgen soll.

ERWEITERTE EINSTELLUNGEN FÜR DIE FIREWALL

Sie können die Arbeit der Firewall zusätzlich anpassen, d.h. den aktiven FTP-Modus zulassen, eine Verbindung blockieren, wenn keine Aktionsanfrage möglich ist (wenn das Programminterface nicht geladen ist), und festlegen, dass die Firewall erst beendet wird, wenn das System vollständig heruntergefahren wird.

In der Grundeinstellung sind diese Parameter deaktiviert.

Gehen Sie folgendermaßen vor, um zusätzliche Parameter für die Firewall festzulegen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

4. Klicken Sie im folgenden Fenster auf der Registerkarte **Paketregeln** auf die Schaltfläche **Erweitert** , um die erweiterten Einstellungen zu öffnen

5. Aktivieren / deaktivieren Sie im folgenden Fenster **Erweitert** die Kontrollkästchen für die entsprechenden Parameter.

SCHUTZ VOR NETZWERKANGRIFFEN

Der Schutz vor Netzwerkangriffen überwacht den eingehenden Datenverkehr auf für Netzwerkangriffe charakteristische Aktivität. Wenn ein Angriffsversuch auf Ihren Computer erkannt wird, blockiert Kaspersky Internet Security jede Art von Netzwerkaktivität des angreifenden Computers im Hinblick auf Ihrem Computer.

In der Grundeinstellung dauert die Blockade eine Stunde. Sie können die Einstellungen für das Blockieren ändern (s. S. 139). Auf dem Bildschirm erscheint eine Meldung über den Angriffsversuch. Die Meldung enthält Informationen über den angreifenden Computer. Beschreibungen der momentan bekannten Netzwerkangriffe (s. Abschnitt "Arten der erkennbaren Netzwerkangriffe" auf S. 137) und entsprechende Abwehrmethoden sind in den Datenbanken von Kaspersky Internet Security enthalten. Die Liste der Angriffe, die der Schutz vor Netzwerkangriffen erkennt, wird im Rahmen des Updates (s. Abschnitt "Update" auf S. 92) der Datenbanken aktualisiert.

IN DIESEM ABSCHNITT

Arten der erkennbaren Netzwerkangriffe 137

Schutz vor Netzwerkangriffen aktivieren und deaktivieren 138

Parameter für das Blockieren ändern 139

ARTEN DER ERKENNBAREN NETZWERKANGRIFFE

Heutzutage existiert einen Vielzahl unterschiedlicher Arten von Netzwerkangriffen. Diese Angriffe nutzen sowohl Schwachstellen des Betriebssystems, als auch installierte System- und Anwendungsprogramme aus.

Um rechtzeitig für die Sicherheit des Computers zu sorgen, ist es wichtig zu wissen, welche Arten von Netzwerkangriffen ihm drohen können. Die bekannten Netzwerkangriffe lassen sich bedingt in drei große Gruppen unterteilen:

- *Scannen von Ports* – Diese Bedrohungsart stellt getrennt betrachtet keinen Angriff dar, sondern geht diesem voraus, weil sie eine der effektivsten Methoden ist, Informationen über einen Remote-Computer zu erhalten. Die Methode besteht darin, die von Netzwerkdiensten auf dem angegriffenen Computer verwendeten UDP/TCP-Ports zu scannen, um deren Status (geschlossene oder offene Ports) zu ermitteln.

  Das Scannen von Ports gibt Aufschluss darüber, welche Angriffstypen für ein bestimmtes System am meisten Erfolg versprechen. Außerdem verleihen die aus dem Scannen resultierenden Informationen ("Abdruck" des Systems) dem Angreifer eine Vorstellung vom Typ des Betriebssystems auf dem entfernten Computer. Dadurch lässt sich die Art der relevanten Angriffe weiter einkreisen und damit die zum Ausführen der Angriffe notwendige Zeit verkürzen. Außerdem können die für das Betriebssystem spezifischen Sicherheitslücken ausgenutzt werden.

- *DoS-Angriffe* oder Angriffe, die zur Dienstverweigerung führen Das Ziel dieser Angriffe besteht darin, die Instabilität des angegriffenen Systems hervorzurufen oder es vollständig außer Gefecht zu setzen. Aufgrund solcher Angriffe können die betroffenen Informationsressourcen unzugänglich werden (z.B. gestörter Internetzugriff).

  Es gibt zwei Haupttypen von DoS-Angriffen:

  - Es werden spezielle Pakete an den angegriffenen Computer geschickt, die dieser nicht erwartet. Die Folge ist eine Überlastung oder ein Systemabsturz.

  - An den angegriffenen Computer wird innerhalb eines kurzen Zeitraums eine große Anzahl von Paketen geschickt, die dieser Computer nicht verarbeiten kann. Als Folge erschöpfen die Systemressourcen.

  Die folgenden Angriffe bieten gute Beispiele für diese Gruppe:

- Der Angriff *Ping of death* besteht im Senden eines ICMP-Pakets, dessen Größe den zulässigen Wert von 64 KB überschreitet. Dieser Angriff kann zum Absturz bestimmter Betriebssysteme führen.

- Bei dem Angriff *Land* wird an einen offenen Port Ihres Computers eine Anfrage auf Verbindungsherstellung mit sich selbst gesendet. Der Angriff führt im angegriffenen Computer zu einer Endlosschleife, was eine stark erhöhte Prozessorbelastung zur Folge hat und bei bestimmten Betriebssystemen zum Absturz führen kann.

- Bei dem Angriff *ICMP Flood* wird eine große Anzahl von ICMP-Paketen an Ihren Computer gesendet Da der Computer auf jedes eintreffende Paket reagieren muss, kommt es zu einer erheblichen Erhöhung der Prozessorauslastung.

- Bei dem Angriff *SYN Flood* wird eine große Menge von Verbindungsanfragen an Ihren Computer gesendet. Das System reserviert für jede dieser Verbindungen bestimmte Ressourcen, wodurch es seine Ressourcen vollständig verbraucht und nicht mehr auf andere Verbindungsversuche reagiert.

- *Angriffe zur "Übernahme"* - Diese Angriffe zielen auf die "Übernahme" des Systems ab. Dies ist der gefährlichste Angriffstyp, weil das System bei erfolgreichem Angriff dem Angreifer gegenüber vollkommen wehrlos ist.

  Dieser Angriff wird benutzt, um von einem Remote-Computer vertrauliche Informationen zu stehlen (beispielsweise Kreditkartennummern und Kennwörter). Ein weiteres Ziel kann darin bestehen, sich im System einzunisten, um später die Rechnerressourcen für die Zwecke des Angreifers zu nutzen (das angegriffene System wird in einem Zombie-Netzwerk oder als "Brückenkopf" für neue Angriffe verwendet).

  Zu dieser Gruppe gehört eine große Anzahl von Angriffen. Sie lassen sich abhängig von dem Betriebssystem, das auf einem Computer installiert ist, in drei Kategorien unterteilen: Angriffe auf Microsoft Windows-Systeme, Angriffe auf Unix-Systeme und eine allgemeine Gruppe für Netzwerkdienste, die in beiden Betriebssystemen verwendet werden.

  Die meistverbreiteten Arten von Angriffen, die auf Netzwerkdienste eines Betriebssystems zugreifen, sind:

  - *Angriffe mit dem Ziel des Pufferüberlaufs*. Ein Pufferüberlauf tritt durch fehlende (oder unzureichende) Kontrolle bei der Arbeit mit Daten-Arrays auf. Dieser Typ von Schwachstellen gehört zu den ältesten und lässt sich am leichtesten von Angreifern ausnutzen.

  - *Angriffe, die auf Fehlern in Formatzeilen beruhen*. Formatzeilenfehler treten auf, weil die Eingabeparameter von Formatfunktionen des Typs *printf(), fprintf(), scanf()* und anderer Standardbibliotheken der Sprache C unzureichend kontrolliert werden. Wenn diese Sicherheitslücke in einem Programm vorhanden ist, kann ein Angreifer die vollständige Kontrolle über das System übernehmen, wenn es ihm gelingt, speziell erstellte Anfragen zu senden.

    Wenn solche Schwachstellen auf dem Benutzercomputer vorhanden sind, werden sie vom Detektionssystem für Angriffe in den gebräuchlichsten Netzwerkdiensten (FTP, POP3, IMAP) automatisch analysiert und ihre Verwendung wird verhindert.

  - *Angriffe, die sich auf das Betriebssystem Microsoft Windows richten,* beruhen auf der Verwendung von Sicherheitslücken der auf einem Computer installierten Software (beispielsweise solcher Programme wie Microsoft SQL Server, Microsoft Internet Explorer, Messenger, sowie Systemkomponenten, die über ein Netzwerk erreichbar sind: DCom, SMB, Wins, LSASS, IIS5).

  Als weiterer häufig anzutreffender Typ von Übernahmeangriffen lässt sich die Verwendung unterschiedlicher Arten von schädlichen Skripts nennen. Dazu zählen auch Skripts, die von Microsoft Internet Explorer verarbeitet werden, sowie die Variationen des Helkern-Wurms. Bei einem Helkern-Angriff werden spezielle UDP-Pakete mit ausführbarem schädlichem Code an einen entfernten Computer gesendet.

SCHUTZ VOR NETZWERKANGRIFFEN AKTIVIEREN UND DEAKTIVIEREN

Der Schutz vor Netzwerkangriffen ist standardmäßig aktiviert und arbeitet im optimalen Modus. Bei Bedarf können Sie den Schutz vor Netzwerkangriffen deaktivieren.

Gehen Sie folgendermaßen vor, um den Schutz vor Netzwerkangriffen zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Schutz vor Netzwerkangriffen**.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **Schutz vor Netzwerkangriffen aktivieren**.

PARAMETER FÜR DAS BLOCKIEREN ÄNDERN

In der Grundeinstellung blockiert der Schutz vor Netzwerkangriffen die Aktivität eines angreifenden Computers für eine Stunde. Sie können das Blockieren für einen bestimmten Computer aufheben oder die Sperrdauer ändern.

Gehen Sie folgendermaßen vor, um den Zeitraum, für den ein angreifender Computer gesperrt werden soll, zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Schutz vor Netzwerkangriffen**.
3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Angreifenden Computer zur Sperrliste hinzufügen für** und legen Sie eine Sperrdauer fest.

Gehen Sie folgendermaßen vor, um einen angreifenden Computer freizugeben:

1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Schutz-Center**.
2. Öffnen Sie auf der rechten Fensterseite durch Linksklick die Komponentenliste **Kontrolle der Arbeit im Netzwerk**.
3. Klicken Sie auf den Link **Netzwerkmonitor**.
4. Wählen Sie im folgenden Fenster **Netzwerkmonitor** auf der Registerkarte **Blockierte Computer** einen blockierten Computer aus und klicken Sie auf **Freigeben**.

UNTERSUCHUNG GESCHÜTZTER VERBINDUNGEN

Eine Verbindung unter Verwendung des SSL/TLS-Protokolls bietet den Schutz des Kommunikationskanals im Internet. Das des SSL/TLS-Protokoll erlaubt die Identifikation der am Datenaustausch beteiligten Partner. Dazu dienen elektronische Zertifikate. Außerdem werden die übertragenen Daten verschlüsselt und beim Übertragungsvorgang wird die Datenintegrität gewährleistet.

Diese Besonderheiten des Protokolls werden aber von Angreifern zur Verbreitung schädlicher Programme benutzt, weil die meisten Antiviren-Produkte den SSL/TLS-Verkehr nicht untersuchen.

Die Untersuchung von geschützten Verbindungen wird in Kaspersky Internet Security mit Hilfe eines Zertifikats von Kaspersky Lab realisiert.

Wenn bei der Verbindung mit einem Server ein inkorrektes Zertifikat gefunden wird (wenn es z.B. von einem ein Angreifer ausgetauscht wurde), erscheint auf dem Bildschirm eine Meldung, in der Sie das Zertifikat akzeptieren oder ablehnen.

Wenn Sie sicher sind, dass die Verbindung mit einer Webseite trotz des inkorrekten Zertifikats immer ungefährlich ist, können Sie die Webseite in die Liste der vertrauenswürdigen Adressen aufnehmen (s. Abschnitt "Liste mit vertrauenswürdigen Adressen erstellen" auf S. 116). Kaspersky Internet Security wird verschlüsselte Verbindungen mit dieser Webseite danach nicht mehr untersuchen.

Sie können den Assistenten für die Zertifikatinstallation verwenden, um eine teilweise interaktive Installation des Zertifikats für die Untersuchung der geschützten Verbindungen in den Browsern Microsoft Internet Explorer, Mozilla Firefox (sofern nicht gestartet) und Google Chrome vorzunehmen und um Anweisungen zur Installation des Kaspersky-Lab-Zertifikats für den Browser Opera zu erhalten.

Gehen Sie folgendermaßen vor, um die Untersuchung von geschützten Verbindungen zu aktivieren und das Kaspersky-Lab-Zertifikat zu installieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** die Komponente **Netzwerk**.
3. Aktivieren Sie im folgenden Fenster das Kontrollkästchen **Geschützte Verbindungen untersuchen**. Bei der ersten Aktivierung dieses Parameters wird der Assistent zur Zertifikatinstallation automatisch gestartet.
4. Klicken Sie auf die Schaltfläche **Zertifikat installieren**, wenn der Assistent nicht gestartet wurde. Es wird ein Assistent gestartet, der Sie bei der Installation des Kaspersky-Lab-Zertifikats unterstützt.

IN DIESEM ABSCHNITT

Untersuchung geschützter Verbindungen in Mozilla Firefox 140

Untersuchung geschützter Verbindungen in Opera 141

UNTERSUCHUNG GESCHÜTZTER VERBINDUNGEN IN MOZILLA FIREFOX

Der Browser Mozilla Firefox verwendet nicht den Zertifikatsspeicher von Microsoft Windows. Bei der Verwendung von Firefox ist es zur Untersuchung von SSL-Verbindungen erforderlich, das Kaspersky-Lab-Zertifikat manuell zu installieren.

Sie können den Assistenten zur Zertifikatinstallation auch verwenden, wenn der Browser nicht gestartet ist.

Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat zu installieren:

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.
3. Wählen Sie im Block **Zertifikate** die Registerkarte **Sicherheit** und klicken Sie auf **Zertifikate anzeigen**.
4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf **Importieren**.
5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Aktivieren Sie im folgenden Fenster die Kontrollkästchen der Aktionen, für deren Untersuchung das installierte Zertifikat verwendet werden soll. Klicken Sie zur Anzeige von Informationen zu dem Zertifikat auf **Anzeigen**.

Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat für Mozilla Firefox Version 3.x zu installieren:

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.
3. Klicken Sie auf der Registerkarte **Verschlüsselung** auf **Zertifikate anzeigen**.
4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf **Importieren**.

5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. Aktivieren Sie im folgenden Fenster die Kontrollkästchen der Aktionen, für deren Untersuchung das installierte Zertifikat verwendet werden soll. Klicken Sie zur Anzeige von Informationen zu dem Zertifikat auf **Anzeigen**.

Wenn Ihr Computer mit dem Betriebssystem Microsoft Windows Vista oder Microsoft Windows 7 arbeitet, lautet der Pfad der Zertifikatsdatei von Kaspersky Lab: *%AllUsersProfile%\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

UNTERSUCHUNG GESCHÜTZTER VERBINDUNGEN IN OPERA

Der Browser Opera verwendet nicht den Zertifikatsspeicher von Microsoft Windows. Bei der Verwendung von Opera ist es zur Untersuchung von SSL-Verbindungen erforderlich, das Kaspersky-Lab-Zertifikat manuell zu installieren.

- *Gehen Sie folgendermaßen vor, das Kaspersky-Lab-Zertifikat zu installieren:*

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Einstellungen**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.

3. Wählen Sie auf der linken Fensterseite die Registerkarte **Sicherheit** und klicken Sie auf **Zertifikate verwalten**.

4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf **Importieren**.

5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. Klicken Sie im folgenden Fenster auf **Installieren**. Das Kaspersky-Lab-Zertifikat wird installiert. Um Informationen zum Zertifikat anzuzeigen und die Aktionen, bei denen das Zertifikat verwendet werden soll, auszuwählen, wählen Sie das Zertifikat in der Liste aus und klicken Sie auf **Anzeigen**.

- *Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat für Opera Version 9.x zu installieren:*

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Einstellungen**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.

3. Wählen Sie auf der linken Fensterseite die Registerkarte **Sicherheit** und klicken Sie auf **Zertifikate verwalten**.

4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf **Importieren**.

5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. Klicken Sie im folgenden Fenster auf **Installieren**. Das Kaspersky-Lab-Zertifikat wird installiert.

Wenn Ihr Computer mit dem Betriebssystem Microsoft Windows Vista oder Microsoft Windows 7 arbeitet, lautet der Pfad der Zertifikatsdatei von Kaspersky Lab: *%AllUsersProfile%\Kaspersky Lab\AVP11\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

NETZWERKMONITOR

Der Netzwerkmonitor dient dazu, in Echtzeit Informationen über die Netzwerkaktivität anzuzeigen.

Gehen Sie folgendermaßen vor, um den Netzwerkmonitor zu starten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Schutz-Center** aus.
2. Öffnen Sie auf der rechten Fensterseite durch Linksklick die Komponentenliste **Kontrolle der Arbeit im Netzwerk**.
3. Klicken Sie auf den Link **Netzwerkmonitor**.

   Das folgende Fenster **Netzwerkmonitor** enthält Informationen über die Netzwerkaktivität.

Bei der Arbeit auf einem Computer mit dem Betriebssystem Microsoft Windows Vista oder Microsoft Windows 7 kann der Netzwerkmonitor mit Hilfe des Kaspersky Gadgets gestartet werden. Dafür kann eine der Schaltflächen des Kaspersky Gadgets mit der Funktion zum Öffnen des Fensters für den Netzwerkmonitor belegt sein (s. Abschnitt "Wie das Kaspersky Gadget verwendet wird" auf S. 78).

Um den Netzwerkmonitor mit Hilfe des Gadgets zu starten,

klicken Sie im Interface von Kaspersky Gadget auf die Schaltfläche mit dem Symbol **Netzwerkmonitor**.

Das folgende Fenster **Netzwerkmonitor** enthält Informationen über die Netzwerkaktivität.

PROXYSERVER-EINSTELLUNGEN

Wenn die Internetverbindung über einen Proxyserver erfolgt, ist es erforderlich, die entsprechenden Verbindungsparameter anzupassen. Kaspersky Internet Security verwendet diese Parameter bei der Arbeit bestimmter Schutzkomponenten und für das Update der Datenbanken und Programm-Module.

Wenn in Ihrem Netzwerk ein Proxyserver installiert ist, der einen nicht standardmäßigen Port benutzt, ist es erforderlich, diesen Port zur Liste der kontrollierten Ports hinzuzufügen (s. Abschnitt "Liste der zu kontrollierenden Ports erstellen" auf S. 142).

Gehen Sie folgendermaßen vor, um die Proxyserver-Parameter anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** die Komponente **Netzwerk**.
3. Klicken Sie im Block **Proxyserver** auf **Proxyserver-Einstellungen anpassen**.
4. Ändern Sie im folgenden Fenster **Proxyserver-Einstellungen** die EInstellungen für den Proxyserver.

LISTE DER ZU KONTROLLIERENDEN PORTS ERSTELLEN

Bei der Arbeit von Schutzkomponenten wie Mail-Anti-Virus, Anti-Spam (s. S. 143), Web-Anti-Virus (auf S. 108) und IM-Anti-Virus werden die Datenströme kontrolliert, die mit bestimmten Protokollen und über bestimmte offene TCP-Ports Ihres Computers übertragen werden. Mail-Anti-Virus analysiert beispielsweise die Informationen, die per SMTP übertragen werden, während Web-Anti-Virus die HTTP-, HTTPS- und FTP-Pakete analysiert.

Sie können die Kontrolle aller oder nur bestimmter Netzwerkports aktivieren. Bei der Kontrolle bestimmter Ports kann eine Liste der Programme angelegt werden, für die alle Ports kontrolliert werden sollen. Es wird empfohlen, in diese Liste Programme aufzunehmen, die Daten per FTP-Protokoll senden oder empfangen.

Gehen Sie folgendermaßen vor, um einen Port zur Liste der kontrollierten Ports hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** die Komponente **Netzwerk**.

3. Wählen Sie im Block **Zu überwachende Ports** die Option **Nur ausgewählte Ports kontrollieren** aus und klicken Sie auf **Auswählen**.

   Das Fenster **Netzwerkports** wird geöffnet.

4. Öffnen Sie über den Link **Hinzufügen**, unterhalb der Portliste im oberen Fensterbereich das Fenster **Netzwerkport** und geben Sie Nummer und Beschreibung des Ports ein.

Gehen Sie folgendermaßen vor, um einen Port aus der Liste der kontrollierten Ports auszuschließen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** die Komponente **Netzwerk**.

3. Wählen Sie im Block **Zu überwachende Ports** die Option **Nur ausgewählte Ports kontrollieren** aus und klicken Sie auf **Auswählen**.

   Das Fenster **Netzwerkports** wird geöffnet.

4. Deaktivieren Sie in der Portliste im oberen Fensterbereich das Kontrollkästchen neben der Beschreibung des Ports, der deaktiviert werden soll.

Gehen Sie folgendermaßen vor, um eine Liste der Programme anzulegen, für die alle Ports kontrolliert werden sollen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** die Komponente **Netzwerk**.

3. Wählen Sie im Block **Zu überwachende Ports** die Option **Nur ausgewählte Ports kontrollieren** aus und klicken Sie auf **Auswählen**.

   Das Fenster **Netzwerkports** wird geöffnet.

4. Aktivieren Sie das Kontrollkästchen **Alle Ports für die angegebenen Programme kontrollieren** und aktivieren Sie in der darunter angeordneten Programmliste die Kontrollkästchen neben den Programmen, für die alle Ports kontrolliert werden sollen.

5. Ist ein Programm nicht in der Liste enthalten, können Sie es wie folgt hinzufügen:

   a. Um die Methode für das Hinzufügen von Programmen in die Liste auszuwählen, öffnen Sie das Menü über den Link **Hinzufügen** unterhalb der Programmliste und wählen Sie einen der folgenden Menüpunkte aus:

      - Wählen Sie den Punkt **Durchsuchen** aus, um den Speicherort der ausführbaren Datei des Programms anzugeben. Nach Auswahl der ausführbaren Datei öffnet sich das Fenster **Programm**.

      - Wählen Sie den Punkt **Programme** aus, um ein Programm aus der Liste der derzeit laufenden Programme auszuwählen. Nach Auswahl eines Programms aus der Liste öffnet sich das Fenster **Programm**.

   b. Geben Sie im Fenster **Programm** eine Beschreibung für das gewählte Programm ein.

ANTI-SPAM

Anti-Spam ist eine spezielle Komponente von Kaspersky Internet Security, die unerwünschte E-Mails (Spam) erkennt und sie nach den Regeln Ihres Mailprogramms verarbeitet. Mit dieser Komponente lässt sich bei der Arbeit mit E-Mails Zeit sparen.

Anti-Spam wird als Erweiterungsmodul in folgende Mailprogramme integriert:

- Microsoft Office Outlook (auf S. 158).

- Microsoft Outlook Express (Windows Mail) (auf. S. 158).
- The Bat! (auf S. 159).
- Thunderbird (auf S. 160).

Legen Sie Listen für erlaubte und verbotene Absender an, um für Anti-Spam festzulegen, von welchen Adressen erwünschte E-Mails bzw. Spam-Mails zu erwarten sind. Als Spam können auch Nachrichten gelten, die nicht an Sie adressiert sind (s. S. 153). Außerdem kann Anti-Spam eine E-Mail auf das Vorhandensein von erlaubten und verbotenen Phrasen sowie von Phrasen aus der Liste für anstößige Ausdrücke analysieren.

Eine Voraussetzung für die effektive Unterscheidung zwischen Spam und nützlichen E-Mails, ist ein Training von Anti-Spam (s. Abschnitt "Anti-Spam-Training" auf S. 146).

Algorithmus für die Arbeit der Komponente

Anti-Spam verwendet einen lernfähigen Algorithmus, mit dem die Komponente mit der Zeit genauer zwischen Spam und erwünschter E-Mails unterscheiden kann. Als Datenquelle für den Algorithmus dient der Inhalt einer E-Mail.

Die Arbeit der Komponente Anti-Spam besteht aus zwei Etappen:

1. Anwendung von strengen Kriterien für die Filterung einer Nachricht. Diese Kriterien ermöglichen es, schnell festzustellen, ob eine Nachricht Spam ist. Anti-Spam weist der Nachricht den Status *Spam* oder *Kein Spam*, die Untersuchung wird beendet und die Nachricht zur Bearbeitung an das Mailprogramm weitergeleitet (siehe unten: Schritte 1–5).
2. Analyse von E-Mails, die nach den strengen Kriterien der vorhergehenden Schritte nicht eingestuft werden konnten. Solche Nachrichten lassen sich nicht eindeutig als Spam bewerten. Deshalb muss Anti-Spam die *Wahrscheinlichkeit* berechnen, mit der es sich bei einer Nachricht um Spam handelt.

Der Algorithmus für die Arbeit von Anti-Spam umfasst folgende Schritte:

1. Es wird geprüft, ob die Absenderadresse einer E-Mail auf den Listen für erlaubte und verbotene Absender steht.
   - Wenn die Absenderadresse in der Liste mit erlaubten Adressen steht, erhält die Nachricht den Status *Kein Spam*.
   - Wenn die Absenderadresse in der Liste mit verbotenen Adressen steht, erhält die Nachricht den Status *Spam*.
2. Wurde die Nachricht mit Hilfe von Microsoft Exchange Server gesendet und die Untersuchung solcher Nachrichten ist deaktiviert, dann erhält sie den Status *Kein Spam*.
3. Die Nachricht wird auf das Vorhandensein von Zeilen aus der Liste mit erlaubten Phrasen analysiert. Wenn mindestens eine Zeile aus dieser Liste gefunden wird, erhält die Nachricht den Status *Kein Spam*. Dieser Schritt wird standardmäßig übersprungen.
4. Es wird analysiert, ob die Nachricht Zeilen aus der Liste der verbotenen Phrasen und der Liste der anstößigen Phrasen enthält. Werden in einer Nachricht Wörter aus diesen Listen gefunden, so werden ihre gewichteten Koeffizienten summiert. Wenn die Summe der Koeffizienten über 100 liegt, erhält die Nachricht den Status *Spam*. Dieser Schritt wird standardmäßig übersprungen.
5. Wenn der Nachrichtentext eine Adresse enthält, die in der Datenbank von verdächtigen oder Phishing-Adressen steht, erhält die Nachricht den Status *Spam*.
6. Die Nachricht wird mit Hilfe heuristischer Regeln analysiert. Wenn aufgrund dieser Analyse in E-Mails typische Spam-Merkmale gefunden werden, erhöht sich die Wahrscheinlichkeit, dass es sich um Spam handelt.
7. Die Nachricht wird mit Hilfe der GSG-Technologie analysiert. Dabei überprüft Anti-Spam die in der E-Mail enthaltenen Bilder. Wenn in den Bildern typische Spam-Merkmale gefunden werden, erhöht sich die Wahrscheinlichkeit, dass es sich um Spam handelt.

8. Dokumente des Formats .rtf, die an eine E-Mail angehängt sind, werden analysiert. Anti-Spam sucht in angehängten Dokumenten nach typischen Spam-Merkmalen. Zum Abschluss der Analyse berechnet Anti-Spam, wie stark sich die Wahrscheinlichkeit erhöht hat, dass es sich bei der Nachricht um Spam handelt. Diese Technologie ist standardmäßig deaktiviert.

9. Das Vorhandensein zusätzlicher Merkmale, die für Spam charakteristisch sind, wird überprüft. Jede Übereinstimmung erhöht die Wahrscheinlichkeit, dass es sich um Spam handelt.

10. Wenn mit Anti-Spam bereits ein Training ausgeführt wurde, wird die Nachricht mit Hilfe der iBayes-Technologie untersucht. Der lernfähige iBayes-Algorithmus berechnet die Wahrscheinlichkeit, mit der es sich bei der Nachricht um Spam handelt. Dazu wird analysiert, wie häufig im Text der Nachricht typische Spam-Phrasen vorkommen.

Die Nachrichtenanalyse ergibt eine Wahrscheinlichkeit, mit der die E-Mail als Spam gilt. Diese Wahrscheinlichkeit wird durch den Wert des *Spam-Faktors* angegeben. Abhängig von den Grenzwerten für den Spam-Faktor wird einer Nachricht der Status *Spam* oder *potentieller Spam* zugewiesen (s. Abschnitt "Grenzwerte für den Spam-Faktor regulieren" auf S. 155). Außerdem wird für Spam und potentiellen Spam im Feld **Betreff** standardmäßig die Markierung **[!! SPAM]** oder **[!! Probable Spam]** (s. Abschnitt "**Markierung zum Betreff einer Nachricht hinzufügen**" auf S. 156) hinzugefügt. Anschließend wird die Nachricht nach den von Ihnen definierten Regeln für Mailprogramme (s. Abschnitt "Spam-Verarbeitung in Mailprogrammen anpassen" auf S. 157) verarbeitet.

IN DIESEM ABSCHNITT

Anti-Spam aktivieren und deaktivieren 145

Stufe für Spam-Schutz wählen 146

Anti-Spam-Training 146

Links in Nachrichten untersuchen 149

Spam nach Phrasen und Adressen ermitteln. Listen erstellen 150

Grenzwerte für den Spam-Faktor regulieren 155

Zusätzliche Merkmale, die den Spam-Faktor beeinflussen, verwenden 155

Algorithmus zur Spam-Erkennung wählen 156

Markierung zum Betreff einer Nachricht hinzufügen 156

Nachrichten für Microsoft Exchange Server von der Untersuchung ausschließen 157

Spam-Verarbeitung in Mailprogrammen anpassen 157

Empfohlene Einstellungen für Anti-Spam wiederherstellen 160

ANTI-SPAM AKTIVIEREN UND DEAKTIVIEREN

Die Komponente kann auf zwei Arten aktiviert und deaktiviert werden.

- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47)

- aus dem Konfigurationsfenster (s. Abschnitt "Programmkonfigurationsfenster" auf S. 52).

Gehen Sie folgendermaßen vor, um Anti-Spam vom Hauptfenster aus zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Schutz-Center**.

2. Öffnen Sie auf der rechten Fensterseite durch Linksklick den Block **Kontrolle der Arbeit im Netzwerk** oder **Schutz für System und Programme**.

3. Klicken Sie auf **Anti-Spam**, um das Menü zur Auswahl einer Aktion für die Komponente zu öffnen, und gehen Sie dort auf **Anti-Spam aktivieren**, um die Komponente zu aktivieren, oder auf Anti-Spam deaktivieren, um die Komponente zu deaktivieren.

   Wird eine Komponente aktiviert, so wird das Symbol links von ihrem Namen grün, wird sie deaktiviert, so wird das Symbol grau.

Gehen Sie folgendermaßen vor, um Anti-Spam vom Konfigurationsfenster aus zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Anti-Spam aktivieren**, um die Komponente einzuschalten. Deaktivieren Sie das Kontrollkästchen, um Anti-Banner auszuschalten.

STUFE FÜR SPAM-SCHUTZ WÄHLEN

Die Auswahl der Spam-Schutzstufe ist davon abhängig, wie häufig Sie Spam erhalten. Die Stufen für den Spam-Schutz entsprechen den Sicherheitsstufen, die von den Kaspersky-Lab-Experten definiert wurden.

- **Hoch**. Diese Sicherheitsstufe sollte verwendet werden, wenn Sie sehr viel Spam erhalten, z.B. bei Verwendung eines kostenlosen Maildiensts. Bei Auswahl dieser Stufe kann die Häufigkeit steigen, dass erwünschte Post als Spam eingestuft wird.

- **Empfohlen**. Diese Sicherheitsstufe gilt für die meisten Situationen als empfohlen.

- **Niedrig**. Diese Sicherheitsstufe sollte verwendet werden, wenn Sie nur selten Spam erhalten, z.B. bei der Arbeit in einer geschützten Umgebung des internen Firmen-Mailsystem. Bei Auswahl dieser Stufe kann die Häufigkeit sinken, dass erwünschte Post als Spam oder potentieller Spam eingestuft wird.

Gehen Sie folgendermaßen vor, um eine der vordefinierten Sicherheitsstufen zu wählen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Wählen Sie auf der rechten Fensterseite mit Hilfe des Schiebereglers die gewünschte Sicherheitsstufe.

   Der Name der gewählten Sicherheitsstufe wird unter der Überschrift des Blocks **Sicherheitsstufe** angezeigt.

Wenn keine der vordefinierten Sicherheitsstufen Ihren Anforderungen entspricht, können Sie die Einstellungen für Anti-Spam anpassen: z.B. die Grenzwerte für den Spam-Faktor ändern oder die Untersuchung von Nachrichten für Microsoft Exchange Server aktivieren. Wenn die Einstellungen verändert werden, ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Um Einstellungsänderungen für Anti-Spam rückgängig zu machen, können Sie die Einstellungen der Komponente wiederherstellen (s. Abschnitt "Empfohlene Einstellungen für Anti-Spam wiederherstellen" auf S. 160).

ANTI-SPAM-TRAINING

Eines der Werkzeuge zur Spam-Erkennung ist der lernfähige iBayes-Algorithmus. Mit diesem Algorithmus wird auf Basis von Phrasen, die in einer Nachricht enthalten sind, darüber entschieden, welchen Status die Nachricht erhält. Bevor der iBayes-Algorithmus eingesetzt wird, benötigt Anti-Spam Zeilenmuster aus erwünschten und aus Spam-Mails. Dazu dient ein *Training.*

Es existieren mehrere Methoden für das Training von Anti-Spam:

- Verwendung eines Trainingsassistenten (Pakettraining). Das Training mit Hilfe des Trainingsassistenten sollte ganz zu Beginn der Arbeit mit Anti-Spam erfolgen.
- Anti-Spam-Training mit ausgehenden E-Mails.
- Training während der Arbeit mit E-Mails in einem Mailprogramm. Dazu dienen für das Training vorgesehene Schaltflächen und Menüpunkte.
- Training bei der Arbeit mit den Anti Spam-Berichten.

IN DIESEM ABSCHNITT

Trainingsassistent verwenden 147

Anti-Spam-Training mit ausgehenden E-Mails 147

Elemente der Benutzeroberfläche eines Mailprogramms verwenden 148

Adressen zur Liste der erlaubten Absender hinzufügen 148

Training mit Berichten 149

TRAININGSASSISTENT VERWENDEN

Der Trainingsassistent erlaubt es, ein Anti-Spam-Training im Paketmodus vorzunehmen. Dazu ist es erforderlich, die Ordner der Benutzerkonten für die Mailprogramme Microsoft Office Outlook und Microsoft Outlook Express (Windows Mail) anzugeben, in denen sich Spam bzw. erwünschte E-Mails befinden.

Für die korrekte Spam-Erkennung ist es erforderlich, ein Training mit mindestens 50 Mustern erwünschter Mails und 50 Spam-Mustern vorzunehmen. Der iBayes-Algorithmus funktioniert nur, wenn die genannten Aktionen ausgeführt wurden.

Um Zeit zu sparen, wird das Training mit dem Assistenten auf 50 Nachrichten aus jedem gewählten Ordner beschränkt.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Gehen Sie folgendermaßen vor, den Assistenten zu starten:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite im Block **Anti-Spam-Training** auf **Trainieren**.

Beim Training mit erwünschten Nachrichten werden die entsprechenden Absenderadressen automatisch zur Liste der erlaubten Absender hinzugefügt. Sie können diese Funktion deaktivieren (s. Abschnitt "Adressen zur Liste der erlaubten Absender hinzufügen" auf S. 148).

ANTI-SPAM-TRAINING MIT AUSGEHENDEN E-MAILS

Sie können Anti-Spam mit 50 ausgehenden E-Mails trainieren. Nachdem das Anti-Spam-Training aktiviert ist, wird jede von Ihnen gesendete Nachricht analysiert und als Muster für eine erwünschte Nachricht verwendet. Das Training wird abgeschlossen, nachdem 50 Nachrichten gesendet wurden.

Gehen Sie folgendermaßen vor, um das Anti-Spam-Training mit ausgehenden E-Mails zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Erweitert** im Block **Ausgehende E-Mails** das Kontrollkästchen **Mit ausgehenden E-Mails trainieren**.

Beim Training mit ausgehenden Nachrichten werden die entsprechenden Empfängeradressen automatisch zur Liste der erlaubten Absender hinzugefügt. Sie können diese Funktion deaktivieren (s. Abschnitt "Adressen zur Liste der erlaubten Absender hinzufügen" auf S. 148).

ELEMENTE DER BENUTZEROBERFLÄCHE EINES MAILPROGRAMMS VERWENDEN

Zum Training von Anti-Spam während der Arbeit mit E-Mails dienen spezielle Elemente auf der Benutzeroberfläche Ihres Mailprogramms (Schaltflächen in der Symbolleiste und Menüpunkte).

Beachten Sie, dass die Schaltflächen und Menüpunkte für das Anti-Spam-Training erst nach der Installation von Kaspersky Internet Security auf der Benutzeroberfläche der Mailprogramme erscheinen.

Gehen Sie folgendermaßen vor, um Anti-Spam mit Hilfe eines Mailprogramms zu trainieren:

1. Starten Sie das Mailprogramm.

2. Wählen Sie eine Nachricht aus, mit deren Hilfe Sie Anti-Spam trainieren möchten.

3. Führen Sie - abhängig davon, welchen Mail-Client Sie verwenden - folgende Aktionen aus:

   - Klicken Sie in der Symbolleiste von Microsoft Office Outlook auf **Spam** oder **Kein Spam**.
   - Klicken Sie in der Symbolleiste von Microsoft Office Outlook (Windows Mail) auf **Spam** oder **Kein Spam**.
   - Verwenden Sie im Mailprogramm The Bat! die dafür vorgesehenen Punkte **Als Spam markieren** und **Als KEIN Spam markieren** im Menü **Extras**.
   - Verwenden Sie in der Symbolleiste von Mozilla Thunderbird die Schaltfläche **Spam/Kein Spam**.

Nachdem eine der oben genannten Aktionen ausgewählt wurde, führt Anti-Spam mit der ausgewählten Nachricht ein Training durch. Wenn Sie mehrere Nachrichten markieren, erfolgt das Training mit allen ausgewählten E-Mails.

Die Absenderadresse einer als erwünscht markierten Nachricht wird automatisch zur Liste der erlaubten Absender hinzugefügt. Sie können diese Funktion deaktivieren (s. Abschnitt "Adressen zur Liste der erlaubten Absender hinzufügen" auf S. 148).

Wenn Sie gleichzeitig mehrere Nachrichten markieren oder sicher sind, dass ein bestimmter Ordner nur Nachrichten einer Gruppe (Spam oder Kein Spam) enthält, kann zum Training der Komponente die Paketmethode mit Hilfe des Trainingsassistenten benutzt werden (s. Abschnitt "Anti-Spam-Training" auf Seite 146).

ADRESSEN ZUR LISTE DER ERLAUBTEN ABSENDER HINZUFÜGEN

Wenn Anti-Spam mit Hilfe des Trainingsassistenten an erwünschten Nachrichten oder direkt im Fenster des Mailprogramms trainiert wird, werden die Absenderadressen von erwünschten Mails automatisch zur Liste der erlaubten Absender hinzugefügt. Dieser Liste werden beim Training mit ausgehenden Nachrichten auch die Empfängeradressen der ausgehenden Mails hinzugefügt.

Sie können diese Funktion deaktivieren, damit die Trainingsergebnisse nicht automatisch zur Liste der erlaubten Absender hinzugefügt werden.

Gehen Sie folgendermaßen vor, damit Adressen nicht zur Liste für erlaubte Absender hinzugefügt werden:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als erwünscht einstufen** das Kontrollkästchen **Von erlaubten Absendern** und klicken Sie auf **Auswählen**.

   Das Fenster **Erlaubte Absender** wird geöffnet.
5. Deaktivieren Sie das Kontrollkästchen **Bei Anti-Spam-Training Adressen von erlaubten Absendern hinzufügen**.

TRAINING MIT BERICHTEN

Es besteht die Möglichkeit, Anti-Spam auf Basis von Berichten zu trainieren. Solche Berichte enthalten Angaben über Nachrichten, die der Kategorie "potentieller Spam" angehören. Beim Training erhalten Nachrichten die Markierung **Spam** oder **Kein Spam** und werden zu den Listen für erlaubte oder verbotene Absender hinzugefügt (s. Abschnitt "Verbotene und erlaubte Absender" auf S. 152).

Gehen Sie folgendermaßen vor, um Anti-Spam an einem Bericht zu trainieren:

1. Öffnen Sie das Programmhauptfenster.
2. Gehen Sie mit Hilfe des Links **Berichte** in das Berichtsfenster von Kaspersky Internet Security.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Detaillierter Bericht**.

   Das Fenster **Detallierter Bericht** wird geöffnet.
4. Wählen Sie auf der linken Fensterseite den Abschnitt **Anti-Spam**.
5. Legen Sie auf der rechten Fensterseite aufgrund der Einträge in der Spalte **Objekt** die Mails fest, an denen Sie Anti-Spam trainieren möchten. Öffnen Sie für jede dieser Nachrichten das Kontextmenü (durch Rechtsklick) und wählen Sie eine entsprechende Aktion für die Nachricht:
   - Als Spam markieren.
   - Als Kein Spam markieren.
   - Zur Erlaubnisliste hinzufügen.
   - Zur Verbotsliste hinzufügen.

LINKS IN NACHRICHTEN UNTERSUCHEN

Anti-Spam kann prüfen, ob die in E-Mails enthaltenen Links auf der Liste verdächtiger Webadressen oder auf der Liste für Phishing-Webadressen stehen. Diese Listen gehören zum Lieferumfang von Kaspersky Internet Security. Wenn ein Phishing-Link oder ein verdächtiger Link in einer Nachricht oder Phishing-Elemente im Nachrichtentext gefunden werden, wird die Nachricht als Spam eingestuft.

Gehen Sie folgendermaßen vor, um die Link-Untersuchung mit den Datenbanken für verdächtige und Phishing-Adressen zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als Spam einstufen** die Kontrollkästchen **Mit Links aus der Datenbank für verdächtige Webadressen** und **Mit Phishing-Elementen**.

SPAM NACH PHRASEN UND ADRESSEN ERMITTELN. LISTEN ERSTELLEN

Sie können folgende Listen erstellen: Listen für erlaubte, verbotene und anstößige Schlüsselphrasen, Listen für erlaubte und verbotene Absenderadressen, Liste für Ihre eigenen Adressen. Beim Einsatz dieser Listen untersucht Anti-Spam den Nachrichteninhalt auf das Vorkommen von Wortverbindungen, die auf der Phrasenliste stehen, und die Absender- und Empfängeradressen auf Übereinstimmungen mit den Einträgen in den Adressenlisten. Wenn eine entsprechende Phrase oder Adresse gefunden wird, identifiziert Anti-Spam die Nachricht - abhängig davon, auf welcher Liste die gefundene Phrase oder Adresse steht - als erwünscht oder als Spam.

Als Spam gelten Nachrichten:

- die verbotene oder anstößige Phrasen mit einem summierten gewichteten Koeffizienten von über 100 enthalten.
- die von einer verbotenen Adresse stammen oder nicht an Sie adressiert sind.

Als erwünscht gelten Nachrichten:

- die erlaubte Phrasen enthalten.
- die von einer erlaubten Adresse stammen.

Masken für Schlüsselphrasen und Absenderadressen

In den Listen für erlaubte, verbotene und anstößige Phrasen können *Masken für Phrasen* verwendet werden. In den Listen für erlaubte und verbotene Absenderadressen sowie in der Liste der vertrauenswürdigen Adressen können *Adressmasken* verwendet werden.

Eine *Maske* ist eine bestimmte Zeile, mit der eine Phrase oder Adresse verglichen wird. Bestimmte Zeichen werden in einer Maske als Platzhalter für andere Zeichen eingesetzt: ***** steht für eine beliebige Zeichenfolge und **?** für ein beliebiges Einzelzeichen. Wenn solche Zeichen in einer Maske verwendet werden, können mehrere Phrasen oder Adressen mit der Maske übereinstimmen (s. folgende Beispiele).

Wenn das Zeichen ***** oder **?** in einer Phrase enthalten ist (z.B. *Wie spät ist es?*), muss ihm das Zeichen **** vorangestellt werden, damit es von Anti-Spam korrekt interpretiert wird. Anstelle des Zeichens ***** muss in der Maske also die Verbindung ***** verwendet werden und anstelle von **?** die Verbindung **\?** (z.B. *Wie spät ist es\?*).

Beispiele für Phrasenmasken:

- *Besuchen Sie unser ** – dieser Maske entspricht eine Nachricht, die mit den Worten *Besuchen Sie unser* beginnt und beliebig fortgeführt wird

Beispiele für Adressmasken:

- *admin@test.com* – Dieser Maske entspricht nur die Adresse *admin@test.com*.
- *admin@** – Dieser Maske entspricht die Adresse eines Absenders mit dem Namen *admin*, z.B. *admin@test.com*, *admin@example.org.*
- **@test** – Dieser Maske entspricht die Adresse eines beliebigen Absenders mit der Mail-Domain *test*, z.B. *admin@test.com*, *info@test.org.*

- *info.*@test.???* – dieser Maske entspricht die Adresse eines beliebigen Absenders einer Nachricht, dessen Name mit *info.* beginnt und dessen Maildomäne mit *test.* anfängt, woraufhin drei beliebige Zeichen folgen, z.B.: *info.product@test.com* oder *info.company@test.org*, nicht jedoch *info.product@test.ru*.

IN DIESEM ABSCHNITT

Verbotene und erlaubte Phrasen 151

Anstößige Phrasen 152

Verbotene und erlaubte Absender 152

Ihre Adressen 153

Phrasen und Adressen exportieren und importieren 153

VERBOTENE UND ERLAUBTE PHRASEN

In der Liste der *verbotenen Phrasen* können Sie Phrasen eintragen, die nach Ihrer Einschätzung für Spam charakteristisch sind, und für jede Phrase einen gewichteten Koeffizienten festlegen. Mit dem *gewichteten Koeffizienten* lässt sich angeben, wie charakteristisch eine Phrase für Spam-Nachrichten ist: Je höher der Koeffizient, desto wahrscheinlicher ist es, dass es sich bei einer Nachricht mit dieser Phrase um Spam handelt. Der gewichtete Koeffizient einer Phrase kann zwischen 0 und 100 liegen. Wenn die Summe der gewichteten Koeffizienten aller in einer Nachricht gefunden Phrasen über 100 liegt, wird die Nachricht als Spam betrachtet.

Schlüsselphrasen, die für erwünschte Nachrichten charakteristisch sind, können in die Liste für *erlaubte Phrasen* aufgenommen werden. Wenn eine solche Phrase in einer Nachricht gefunden wird, identifiziert Anti-Spam diese als erwünscht (Kein Spam).

In die Listen für verbotene und erlaubte Phrasen können vollständige Adressen und entsprechende Masken eingetragen werden (s. Abschnitt "Spam nach Phrasen und Adressen ermitteln. Listen erstellen" auf S. 150).

Gehen Sie folgendermaßen vor, um eine Liste mit verbotenen oder erlaubten Absendern zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Gehen Sie auf der Registerkarte **Allgemein** folgendermaßen vor:

   - Wenn eine Liste für verbotene Phrasen erstellt werden soll, aktivieren Sie im Block **Folgende Nachrichten als Spam einstufen** das Kontrollkästchen **Mit verbotenen Phrasen** und klicken Sie rechts auf **Auswählen**.

     Das Fenster **Verbotene Phrasen** wird geöffnet.

   - Wenn eine Liste für erlaubte Phrasen erstellt werden soll, aktivieren Sie im Block **Folgende Nachrichten als erwünscht einstufen** das Kontrollkästchen **Mit erlaubten Phrasen** und klicken Sie rechts auf **Auswählen**.

     Das Fenster **Erlaubte Phrasen** wird geöffnet.
5. Öffnen Sie mit dem Link **Hinzufügen** das Fenster **Verbotene Phrase** (oder das Fenster **Erlaubte Phrase**).
6. Geben Sie eine vollständige Phrase oder eine entsprechende Maske ein, legen Sie einen gewichteten Koeffizienten für die verbotene Phrase fest und klicken Sie anschließend auf **OK**.

Damit eine bestimmte Maske nicht mehr verwendet wird, muss sie nicht gelöscht werden. Es ist ausreichend, im Fenster mit der Liste das entsprechende Kontrollkästchen zu deaktivieren.

ANSTÖßIGE PHRASEN

Im Lieferumfang von Kaspersky Internet Security befindet sich eine Liste mit anstößigen Phrasen, die Spezialisten von Kaspersky Lab erstellt haben. Die Liste enthält anstößige Phrasen, deren Vorhandensein in einer Nachricht mit großer Wahrscheinlichkeit darauf hinweist, dass es sich um Spam handelt. In diese Listen können vollständige Phrasen und entsprechende Masken eingetragen werden (s. Abschnitt "Spam nach Phrasen und Adressen ermitteln. Listen erstellen" auf S. 150).

Wenn für einen Benutzer die Kindersicherung (s. S. 169) aktiviert ist und die Einstellungen der Kindersicherung durch ein Kennwort geschützt sind, ist das Kennwort (s. S. 83) erforderlich, um die Liste für anstößige Phrasen zu öffnen.

Gehen Sie folgendermaßen vor, um die Liste der anstößigen Phrasen zu bearbeiten:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als Spam einstufen** das Kontrollkästchen **Mit verbotenen Phrasen** und klicken Sie auf **Auswählen**.

   Das Fenster **Verbotene Phrasen** wird geöffnet.
5. Aktivieren Sie das Kontrollkästchen **Anstößige Phrasen als verboten einstufen** und öffnen Sie mit dem Link **anstößige Phrasen** das Fenster **Vereinbarung**.
6. Lesen Sie den Vereinbarungstext. Wenn Sie den genannten Bedingungen zustimmen, aktivieren Sie unten das Kontrollkästchen und klicken Sie auf **OK**.

   Das Fenster **Anstößige Lexik** wird geöffnet.
7. Öffnen Sie mit dem Link **Hinzufügen** das Fenster **Verbotene Phrase**.
8. Geben Sie eine vollständige Phrase oder eine entsprechende Maske ein, legen Sie einen gewichteten Koeffizienten für die Phrase fest und klicken Sie auf **OK**.

Damit eine bestimmte Maske nicht mehr verwendet wird, muss sie nicht gelöscht werden. Es ist ausreichend, im Fenster **Anstößige Lexik** das entsprechende Kontrollkästchen zu deaktivieren.

VERBOTENE UND ERLAUBTE ABSENDER

Zur Liste der *verbotenen Absender* können Sie Absenderadressen hinzufügen, deren Nachrichten von Anti-Spam als Spam identifiziert wurden. Absenderadressen, von denen kein Spam erwartet wird, stehen auf der Liste der *erlaubten Absender*. Diese Liste wird beim Training der Komponente Anti-Spam (s. Abschnitt "Adressen zur Liste der erlaubten Absender hinzufügen" auf S. 148) automatisch angelegt. Außerdem können Sie der Liste Einträge hinzufügen.

In die Listen für erlaubte und verbotene Absender können vollständige Adressen und Adressmasken eingetragen werden (s. Abschnitt "Spam nach Phrasen und Adressen ermitteln. Listen erstellen" auf S. 150).

Gehen Sie folgendermaßen vor, um eine Liste mit erlaubten oder verbotenen Absendern zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.

4. Gehen Sie auf der Registerkarte **Allgemein** folgendermaßen vor:

   - Wenn eine Liste für verbotene Absender erstellt werden soll, aktivieren Sie im Block **Folgende Nachrichten als Spam einstufen** das Kontrollkästchen **Von verbotenen Absendern** und klicken Sie rechts auf **Auswählen**.

     Das Fenster **Verbotene Absender** wird geöffnet.

   - Wenn eine Liste für erlaubte Absender erstellt werden soll, aktivieren Sie im Block **Folgende Nachrichten als erwünscht einstufen** das Kontrollkästchen **Von erlaubten Absendern** und klicken Sie rechts auf **Auswählen**.

     Das Fenster **Erlaubte Absender** wird geöffnet.

5. Öffnen Sie mit dem Link **Hinzufügen** das Fenster **Adressmaske für E-Mails**.

6. Geben Sie eine Adressmaske ein und klicken Sie auf **OK**.

Damit eine bestimmte Maske nicht mehr verwendet wird, muss sie nicht gelöscht werden. Es ist ausreichend, im Fenster mit der Liste das entsprechende Kontrollkästchen zu deaktivieren.

IHRE ADRESSEN

Sie können eine Liste mit Ihren E-Mail-Adressen anlegen, damit nicht an Sie adressierte Mails als Spam markiert werden

Gehen Sie folgendermaßen vor, um eine Liste mit Ihren Adressen anzulegen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen **Nicht an mich adressiert** und klicken Sie auf **Meine Adressen**.

   Das Fenster **Meine Adressen** wird geöffnet.

5. Öffnen Sie mit dem Link **Hinzufügen** das Fenster **Adressmaske für E-Mails**.

6. Geben Sie eine Adressmaske ein und klicken Sie auf **OK**.

Damit eine bestimmte Maske nicht mehr verwendet wird, muss sie nicht gelöscht werden. Es ist ausreichend, im Fenster **Meine Adressen** das entsprechende Kontrollkästchen zu deaktivieren.

PHRASEN UND ADRESSEN EXPORTIEREN UND IMPORTIEREN

Listen mit Phrasen und Adressen können flexibel eingesetzt werden. Zum Beispiel können Adressen in eine entsprechende Liste auf einem anderen Computer übertragen werden, auf dem Kaspersky Internet Security installiert ist.

Dabei gilt folgendes Vorgehen:

1. *Exportieren* Sie eine Liste, d.h. die Einträge werden aus einer Liste in eine Datei kopiert.

2. Übertragen Sie die gespeicherte Datei auf einen anderen Computer (z.B. per E-Mail oder mit einem Wechseldatenträger).

3. *Importieren* Sie eine Liste, d.h. die Einträge werden aus einer Datei in eine analoge Liste auf einem anderen Computer eingetragen.

Beim Export einer Liste können Sie wählen, ob nur ausgewählte Listenelemente oder die gesamte Liste kopiert werden soll. Beim Import können der Liste neue Elemente hinzugefügt oder die vorhandene Liste durch eine importierte ersetzt werden.

Gehen Sie folgendermaßen vor, um die Einträge aus einer Liste zu exportieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen in der Zeile mit dem Namen der Liste, aus der die Einträge exportiert werden sollen. Klicken Sie dann rechts auf die entsprechende Schaltfläche.

5. Aktivieren Sie im folgenden Fenster in der Liste die Kontrollkästchen für die Einträge, die in die Datei aufgenommen werden sollen.

6. Klicken Sie auf den Link **Export**.

   Im folgenden Fenster können Sie wählen, welche Elemente exportiert werden sollen. Führen Sie hier eine der folgenden Aktionen aus:

   - Klicken Sie auf **Ja**, wenn nur ausgewählte Einträge in die Datei aufgenommen werden sollen.

   - Klicken Sie auf **Nein**, wenn die gesamte Liste aufgenommen werden soll.

7. Geben Sie im folgenden Fenster einen Typ und einen Namen für die zu speichernde Datei an und bestätigen Sie das Speichern.

Gehen Sie folgendermaßen vor, um die Einträge aus einer Datei in eine Liste zu importieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen in der Zeile mit dem Namen der Liste, in den die Einträge importiert werden sollen. Klicken Sie dann rechts auf die entsprechende Schaltfläche.

5. Klicken Sie im Fenster auf den Link **Import**. Wenn Sie eine Liste mit erlaubten Absendern importieren, wählen Sie im folgenden Menü den Punkt **Aus Datei importieren**. Für die übrigen Listen muss kein Menüpunkt gewählt werden.

   Wenn die Liste nicht leer ist, wird Ihnen im folgenden Fenster vorgeschlagen, die zu importierenden Elemente hinzuzufügen. Führen Sie hier eine der folgenden Aktionen aus:

   - Klicken Sie auf **Ja**, wenn die Dateieinträge zur Liste hinzugefügt werden sollen.

   - Klicken Sie auf **Nein**, wenn die vorhandenen Einträge durch die Liste aus der Datei ersetzt werden sollen.

6. Wählen Sie im folgenden Fenster eine Datei mit den zu importierenden Einträgen.

Liste mit erlaubten Absendern aus einem Adressbuch importieren

Für Adressen aus der Liste erlaubter Absender ist der Import von Adressen oder eines Adressbuchs für Microsoft Office Outlook / Microsoft Outlook Express (Windows Mail) möglich.

Gehen Sie folgendermaßen vor, um eine Liste mit erlaubten Absendern aus einem Adressbuch zu importieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als erwünscht einstufen** das Kontrollkästchen **Von erlaubten Absendern** und klicken Sie auf **Auswählen**.

   Das Fenster **Erlaubte Absender** wird geöffnet.
5. Klicken Sie auf den Link **Import**, öffnen Sie das Menü zur Auswahl einer Quelle und wählen Sie den Punkt **Aus Adressbuch importieren**.
6. Wählen Sie im folgenden Fenster das entsprechende Adressbuch.

GRENZWERTE FÜR DEN SPAM-FAKTOR REGULIEREN

Die Spam-Erkennung basiert auf der Verwendung moderner Filtertechnologien, die es erlauben, Anti-Spam so zu trainieren (s. Abschnitt "Anti-Spam-Training" auf S. 146), dass er relativ genau zwischen Spam, potentiellem Spam und erwünschten Mails unterscheiden kann. Dabei erhält jedes Element einer erwünschten oder einer Spam-Mail einen Koeffizienten.

Wenn eine E-Mail in Ihrer Mailbox eintrifft, untersucht Anti-Spam die Nachricht mit Hilfe der iBayes-Technologie auf das Vorhandensein von Elementen, die für Spam und erwünschte Post charakteristisch sind. Die Koeffizienten für jedes Element einer erwünschten oder einer Spam-Mail werden summiert, und ein *Spam-Faktor* wird errechnet. Je höher der Spam-Faktor, desto höher ist die Wahrscheinlichkeit, mit der es sich bei einer Nachricht um Spam handelt. In der Grundeinstellung gilt eine Nachricht mit einem Spam-Faktor bis 60 als erwünscht. Bei einem Spam-Faktor von über 60 gilt eine Nachricht als potentieller Spam. Wenn der Wert über 90 liegt, wird eine Nachricht als Spam betrachtet. Sie können die Grenzwerte für den Spam-Faktor ändern.

Gehen Sie folgendermaßen vor, um die Grenzwerte für den Spam-Faktor zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Passen Sie auf der Registerkarte **Algorithmus** im Block **Spam-Faktor** den Wert des Spam-Faktors an. Dazu dient der Schieberegler oder das Eingabefeld mit Pfeiltasten.

ZUSÄTZLICHE MERKMALE, DIE DEN SPAM-FAKTOR BEEINFLUSSEN, VERWENDEN

Das Ergebnis für den Spam-Faktor kann durch zusätzliche Nachrichtenmerkmale beeinflusst werden: beispielsweise das Fehlen einer Empfängeradresse im Feld "An" oder eine zu lange Betreffzeile (über 250 Zeichen). Wenn eine Nachricht diese Merkmale aufweist, erhöht sich die Wahrscheinlichkeit, dass es sich um Spam handelt. Der Wert für den Spam-

Faktor erhöht sich entsprechend. Sie können wählen, welche Zusatzmerkmale bei der Nachrichtenanalyse berücksichtigt werden sollen.

Gehen Sie folgendermaßen vor, um Zusatzmerkmale zu verwenden, die den Spam-Faktor erhöhen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Klicken Sie auf der Registerkarte **Algorithmus** auf **Erweitert**.
5. Aktivieren Sie im folgenden Fenster **Erweitert** das Kontrollkästchen für die Merkmale, die bei der Nachrichtenanalyse berücksichtigt werden sollen, um den Spam-Faktor zu erhöhen.

ALGORITHMUS ZUR SPAM-ERKENNUNG WÄHLEN

Die Spam-Analyse von E-Mails erfolgt unter Verwendung von Algorithmen zum Erkennen.

- **Heuristische Analyse**. Anti-Spam analysiert die Nachrichten mit Hilfe heuristischer Regeln. Die heuristische Analyse wird immer verwendet.
- **Grafikanalyse (GSG)**. Die GSG-Technologie wird von Anti-Spam verwendet, um Spam in Form von Bildern zu identifizieren.
- **Analyse von angehängten Dokumenten im Format rtf**. Anti-Spam analysiert die an Nachrichten angehängten Dokumente auf das Vorhandensein von Spam-Merkmalen.
- **Lernfähiger Algorithmus zur Textanalyse (iBayes)**. Mit dem iBayes-Algorithmus wird analysiert, wie häufig im Text einer Nachricht Wörter verwendet werden, die für Spam typisch sind. Aufgrund der Analyse wird eine Nachricht als erwünscht oder als Spam eingestuft. Vor der Verwendung des iBayes-Algorithmus ist ein Anti-Spam-Training erforderlich (s. Abschnitt "Anti-Spam-Training" auf S. 146).

Gehen Sie folgendermaßen vor, um bei der E-Mail-Analyse einen Spam-Erkennungsalgorithmus zu verwenden / nicht zu verwenden:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Aktivieren / deaktivieren Sie auf der Registerkarte **Algorithmus** im Block **Erkennungsalgorithmen** die entsprechenden Kontrollkästchen.

MARKIERUNG ZUM BETREFF EINER NACHRICHT HINZUFÜGEN

Anti-Spam kann Nachrichten, die sich bei der Untersuchung als Spam oder potentieller Spam erweisen, im Feld **Betreff** spezielle Markierungen hinzufügen:

- **[!! SPAM]** – für Nachrichten, die als Spam identifiziert wurden.
- **[?? Probable Spam]** – für Nachrichten, die als potentieller Spam identifiziert wurden.

Solche Markierungen in der Betreffzeile können Ihnen bei der Durchsicht von Nachrichtenlisten behilflich sein, Spam und potentiellen Spam aufzufinden.

Gehen Sie folgendermaßen vor, damit Anti-Spam der Betreffzeile Markierungen hinzufügt / nicht hinzufügt:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Erweitert** im Block **Aktionen** die Kontrollkästchen für die Markierungen, die dem Betreff hinzugefügt werden sollen. Wenn ein Kontrollkästchen angekreuzt wurde, kann der Markierungstext geändert werden. Deaktivieren Sie das entsprechende Kontrollkästchen, wenn keine Markierung erforderlich ist.

NACHRICHTEN FÜR MICROSOFT EXCHANGE SERVER VON DER UNTERSUCHUNG AUSSCHLIEßEN

Sie können E-Mails, die im Rahmen eines internen Netzwerks (z.B. Firmenpost) verschickt werden, von der Spam-Untersuchung ausschließen. Beachten Sie, dass dann E-Mails als interne Mail betrachtet werden, wenn als Mail-Client auf allen Netzwerkcomputern das Programm Microsoft Office Outlook benutzt wird und die Mailboxen der Benutzer sich auf einem Exchange-Server oder auf den Servern, die mit X400-Konnektoren verbunden sind, befinden.

In der Grundeinstellung werden Nachrichten für Microsoft Exchange Server nicht von Anti-Spam untersucht.

Gehen Sie folgendermaßen vor, damit Anti-Spam die Nachrichten für Microsoft Exchange Server analysiert:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Deaktivieren Sie auf der Registerkarte im Block **Ausnahmen** das Kontrollkästchen **E-Mails für Microsoft Exchange Server nicht untersuchen**.

SPAM-VERARBEITUNG IN MAILPROGRAMMEN ANPASSEN

Wenn sich aufgrund einer Untersuchung ergibt, dass eine Nachricht als Spam oder potentieller Spam gilt, sind die weiteren Aktionen von Anti-Spam vom Status der Nachricht und von der gewählten Aktion abhängig. Standardmäßig werden E-Mails, die als Spam oder potentieller Spam gelten, modifiziert: Einer Nachricht wird im Feld **Betreff** die Markierung **[!! SPAM]** oder **[?? Probable Spam]** hinzugefügt (s. Abschnitt "Markierung zum Betreff einer Nachricht hinzufügen" auf S. 156).

Sie können Zusatzaktionen für Spam und potentiellen Spam festlegen. In den Mailprogrammen Microsoft Office Outlook und Microsoft Outlook Express (Windows Mail) sind dafür spezielle Erweiterungsmodule vorgesehen. Für die Mailprogramme The Bat! und Thunderbird können Sie Filterregeln erstellen.

IN DIESEM ABSCHNITT

Microsoft Office Outlook 158

Microsoft Outlook Express (Windows Mail) 158

Regel für die Spam-Untersuchung von Nachrichten erstellen 158

The Bat! 159

Thunderbird 160

MICROSOFT OFFICE OUTLOOK.

E-Mails, die Anti-Spam als Spam oder potentieller Spam klassifiziert, werden im Feld **Betreff** standardmäßig durch die Markierungen **[!! SPAM]** oder **[?? Probable Spam]** gekennzeichnet. Wenn es erforderlich ist, Nachrichten nach der Untersuchung durch Anti-Spam zusätzlich zu verarbeiten, können Sie Microsoft Office Outlook entsprechend anpassen. Das Einstellungsfenster für die Spam-Bearbeitung erscheint automatisch, wenn das Mailprogramm nach der Installation von Kaspersky Internet Security zum ersten Mal gestartet wird. Die Parameter für die Verarbeitung von Spam und potentiellen Spam stehen außerdem in Microsoft Office Outlook auf der speziellen Registerkarte **Anti-Spam** im Menü **Extras** → **Optionen** zur Verfügung.

MICROSOFT OUTLOOK EXPRESS (WINDOWS MAIL).

E-Mails, die Anti-Spam als Spam oder potentieller Spam klassifiziert, werden im Feld **Betreff** standardmäßig durch die Markierungen **[!! SPAM]** oder **[?? Probable Spam]** gekennzeichnet. Wenn es erforderlich ist, Nachrichten nach der Untersuchung durch Anti-Spam zusätzlich zu verarbeiten, können Sie Microsoft Office Outlook (Windows Mail) entsprechend anpassen.

Das Einstellungsfenster für die Spam-Verarbeitung erscheint, wenn das Mailprogramm nach der Installation der Anwendung zum ersten Mal gestartet wird. Es kann auch mit der Schaltfläche **Einstellungen** geöffnet werden, die sich neben den Schaltflächen **Spam** und **Kein Spam** auf der Symbolleiste befindet.

REGEL FÜR DIE SPAM-UNTERSUCHUNG VON NACHRICHTEN ERSTELLEN

Im Folgenden wird erklärt, wie Spam-Regeln für die Nachrichtenverarbeitung mit Anti-Spam im Mailprogramm Microsoft Office Outlook erstellt werden. Auf Basis dieser Anleitung können Sie eine eigene Regel erstellen.

Gehen Sie folgendermaßen vor, um eine Regel zur Spam-Verarbeitung von Nachrichten zu erstellen:

1. Starten Sie das Programm Microsoft Office Outlook und verwenden Sie den Befehl **Extras** →**Regeln und Benachrichtigungen** im Programmhauptfenster. Die Methode für den Start des Assistenten ist von der Microsoft Office Outlook-Version abhängig, die Sie verwenden. In dieser Hilfe wird das Erstellen einer Regel mit Hilfe von Microsoft Office Outlook 2003 beschrieben.

2. Gehen Sie im Fenster **Regeln und Benachrichtigungen** auf die Registerkarte **Regeln für E-Mails** und klicken Sie auf **Neu**. Dadurch wird der Assistent zum Erstellen einer neuen Regel gestartet. Er besteht aus einer Folge von Fenstern / Schritten:

   a. Sie können wählen, ob zum Erstellen der Regel eine Vorlage benutzt werden soll oder nicht. Wählen Sie die Variante **Regel ohne Vorlage erstellen** und wählen Sie als Prüfungsbedingung **Nachrichten bei Ankunft prüfen**. Klicken Sie auf **Weiter**.

   b. Klicken Sie im Fenster zur Auswahl der Bedingungen für die Nachrichtenprüfung auf **Weiter**, ohne ein Kontrollkästchen zu aktivieren. Bestätigen Sie in der Bestätigungsanfrage die Anwendung dieser Regel auf alle Nachrichten, die Sie erhalten.

c. Aktivieren Sie im Fenster zur Auswahl der Aktionen für die Nachrichten in der Aktionsliste das Kontrollkästchen **diese mit einer vordefinierten Aktion bearbeiten**. Klicken Sie im unteren Bereich des Fensters auf den Link **einer vordefinierten Aktion**. Wählen Sie aus der Dropdown-Liste den Wert **Kaspersky Anti-Spam** und klicken Sie auf **OK**.

d. Klicken Sie im Fenster zur Auswahl von Ausnahmen auf **Weiter**, ohne ein Kontrollkästchen zu aktivieren.

e. Im Fenster zum Abschluss der Regelerstellung können Sie den Namen der Regel ändern (standardmäßig lautet er Kaspersky Anti-Spam). Überprüfen Sie, ob das Kontrollkästchen **Diese Regel aktivieren** aktiviert ist und klicken Sie auf **Fertig**.

3. Die neue Regel wird standardmäßig an erste Stelle zur Regelliste im Fenster **Regeln und Benachrichtigungen** hinzugefügt. Wenn Sie möchten, dass die Regel zuletzt auf eine Nachricht angewandt wird, verschieben Sie sie an das Ende der Liste.

Alle Nachrichten, die in der Mailbox ankommen, werden auf der Grundlage von Regeln bearbeitet. Die Verwendungsreihenfolge der Regeln hängt von der Priorität ab, die den einzelnen Regeln zugewiesen wurde. Die Regeln werden nacheinander verwendet, wobei mit der obersten Regel begonnen wird und die Priorität der Regeln nach unten sinkt. Sie können die Anwendungspriorität der Regeln für Nachrichten erhöhen oder senken. Dazu wird eine Regel in der Liste nach oben oder unten verschoben. Wenn Sie nicht möchten, dass eine Nachricht zusätzlich nach einer Anti-Spam-Regel bearbeitet wird, nachdem bereits eine Regel angewandt wurde, muss in den Parametern dieser Regel das Kontrollkästchen **keine weiteren Regeln anwenden** aktiviert werden (s. Schritt 3. zum Erstellen der Regel).

THE BAT!

Die Aktionen für Spam und potentiellen Spam werden im Mailprogramm The Bat! mit den Mitteln des Mailprogramms festgelegt.

➧ *Gehen Sie folgendermaßen vor, um in The Bat! die Spam-Verarbeitungsregeln anzupassen:*

1. Wählen Sie im Menü **Optionen** des Mailprogramms den Punkt **Benutzereinstellungen**.

2. Wählen Sie in der Konfigurationsstruktur das Objekt **Spam-Schutz**.

Die angezeigten Parameter für den Spam-Schutz gelten für alle auf dem Computer installierten Anti-Spam-Module, die die Arbeit mit The Bat! unterstützen.

Sie müssen eine Score-Stufe festlegen und die Aktion angeben, die auf Nachrichten angewandt werden soll, denen ein bestimmter Score zugewiesen wurde (im Fall von Anti-Spam ist das die Wahrscheinlichkeit, dass eine E-Mail als Spam gilt):

- Nachricht mit einem Score, der den Grenzwert überschreitet, löschen.
- Nachricht mit einem bestimmten Score in einen speziellen Ordner für Spam-Nachrichten verschieben.
- Spam-Nachrichten, die mit einer speziellen Kopfzeile markiert sind, in den Spam-Ordner verschieben.
- Spam-Nachrichten im Ordner **Eingang** belassen.

Aufgrund der Bearbeitung von E-Mail-Nachrichten durch Kaspersky Internet Security wird der Nachricht auf der Basis eines Faktors, den Sie festlegen können, der Status Spam oder potentieller Spam zugewiesen. Im Mailprogramm The Bat! ist ein entsprechender Score-Algorithmus für Nachrichten realisiert, der den Gegenstand Spam betrifft, und ebenfalls auf dem Spam-Faktor basiert. Um Differenzen zwischen den Spam-Faktoren in Kaspersky Internet Security und in The Bat! zu vermeiden, werden alle von Anti-Spam geprüften Nachrichten dem Rating angepasst, das dem Status der Nachricht entspricht: erwünschte E-Mails – 0%, potentieller Spam – 50%, Spam – 100%. Dadurch stimmt der Score der Nachricht im Mailprogramm The Bat! nicht mit dem in Anti-Spam festgelegten Spam-Faktor überein, sondern mit dem Faktor des entsprechenden Status.

Einzelheiten über den Spam-Score und die Verarbeitungsregeln s. Dokumentation zum Mailprogramm The Bat!.

THUNDERBIRD.

E-Mails, die Anti-Spam als Spam oder potentieller Spam klassifiziert, werden im Feld **Betreff** standardmäßig durch die Markierungen **[!! SPAM]** oder **[?? Probable Spam]** gekennzeichnet. Wenn nach der Untersuchung durch Anti-Spam eine zusätzliche Nachrichtenverarbeitung erforderlich ist, können Sie Thunderbird entsprechend anpassen. Öffnen Sie dazu mit dem Menübefehl **Extras** → **Filter** das Konfigurationsfenster (Details über die Arbeit mit dem Mail-Client s. Hilfe zu Mozilla Thunderbird).

Das Anti-Spam-Erweiterungsmodul für Thunderbird erlaubt es, ein Training mit E-Mails vorzunehmen, die mit diesem Mail-Client empfangen und gesendet wurden. Außerdem kann die E-Mail-Korrespondenz auf Spam untersucht werden. Das Modul wird in Thunderbird integriert und leitet E-Mails zur Untersuchung an die Komponente Anti-Spam um. Dazu dient der Menübefehl **Extras** → **Junk-Filter auf Ordner anwenden**. Die Nachrichtenuntersuchung wird also nicht von Thunderbird, sondern von Kaspersky Internet Security ausgeführt. Dabei bleibt die Funktionalität von Thunderbird unverändert.

Der Status des Anti-Spam-Erweiterungsmoduls wird in Form eines Symbols in der Statuszeile von Thunderbird angezeigt. Das graue Symbol bedeutet, dass bei der Arbeit des Plug-ins ein Problem vorliegt oder dass die Komponente Anti-Spam deaktiviert wurde. Das Konfigurationsfenster von Kaspersky Internet Security kann durch Doppelklick auf das Symbol geöffnet werden. Um zu den Einstellungen für Anti-Spam zu gelangen, klicken Sie im Block **Anti-Spam** auf **Einstellungen.**

EMPFOHLENE EINSTELLUNGEN FÜR ANTI-SPAM WIEDERHERSTELLEN

Um Einstellungsänderungen für Anti-Spam rückgängig zu machen, können Sie die von Kaspersky Lab empfohlenen Einstellungen wiederherstellen, die der Sicherheitsstufe **Empfohlen** entsprechen.

Gehen Sie folgendermaßen vor, um die standardmäßigen Einstellungen für den Schutz vor unerwünschten E-Mails wiederherzustellen,

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Standard**.

   Die Sicherheitsstufe erhält den Wert **Empfohlen**.

ANTI-BANNER

Anti-Banner dient dazu, die Anzeige von Bannern auf den von Ihnen besuchten Webseiten und im Interface bestimmter Computerprogramme zu blockieren. Bannerwerbung kann Sie von der Arbeit ablenken und verursacht erhöhten Datenverkehr.

Bevor ein Banner auf einer Webseite oder im Fenster eines Computerprogramms angezeigt wird, muss es aus dem Internet geladen werden. Anti-Banner prüft die Adresse, von der ein Banner geladen wird. Stimmt die Adresse mit einer Maske aus der im Lieferumfang von Kaspersky Internet Security enthaltenen Liste oder der von Ihnen angelegten Schwarzen Bannerliste überein, dann wird das Banner blockiert. Zum Sperren von Bannern, deren Adressmasken nicht in den genannten Listen enthalten sind, wird eine heuristische Analyse verwendet (s. Abschnitt "Untersuchungsmethoden wählen" auf S. 162).

Zusätzlich kann eine Weiße Adressenliste angelegt werden, auf deren Basis die Banneranzeige erlaubt wird.

IN DIESEM ABSCHNITT

Anti-Banner aktivieren und deaktivieren 161

Untersuchungsmethoden wählen 162

Listen für verbotene und erlaubte Banneradressen erstellen 162

Adressenlisten exportieren / importieren 162

ANTI-BANNER AKTIVIEREN UND DEAKTIVIEREN

Anti-Banner ist nach der Installation von Kaspersky Internet Security deaktiviert und blockiert die Banneranzeige nicht. Um das Blockieren von Bannern einzuschalten, muss Anti-Banner aktiviert werden.

Damit alle Banner angezeigt werden, muss Anti-Banner deaktiviert werden. Wenn nur die Anzeige bestimmter Banner erlaubt werden soll, verwenden Sie die Liste der erlaubten Banneradressen (s. Abschnitt "Listen für verbotene und erlaubte Banneradressen erstellen" auf S. 162).

Die Komponente kann auf zwei Arten aktiviert und deaktiviert werden.

- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47)
- aus dem Konfigurationsfenster (s. Abschnitt "Programmkonfigurationsfenster" auf S. 52).

Gehen Sie folgendermaßen vor, um Anti-Banner vom Hauptfenster aus zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Schutz-Center**.
2. Öffnen Sie auf der rechten Fensterseite durch Linksklick den Block **Kontrolle der Arbeit im Netzwerk**.
3. Klicken Sie auf **Anti-Banner**, um das Menü zur Auswahl einer Aktion für die Komponente zu öffnen, und gehen Sie dort auf **Anti-Banner aktivieren**, um die Komponente zu aktivieren, oder auf Anti-Banner deaktivieren, um die Komponente zu deaktivieren.

   Wird eine Komponente aktiviert, so wird das Symbol links von ihrem Namen grün, wird sie deaktiviert, so wird das Symbol grau.

Gehen Sie folgendermaßen vor, um Anti-Banner vom Konfigurationsfenster aus zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Banner**.
3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Anti-Banner aktivieren**, um die Komponente einzuschalten. Deaktivieren Sie das Kontrollkästchen, um Anti-Banner auszuschalten.

UNTERSUCHUNGSMETHODEN WÄHLEN

Sie können die Methoden festlegen, mit denen Anti-Banner Adressen untersuchen soll, von denen Banner geladen werden können: Zusätzlich zu diesen Methoden untersucht Anti-Banner die Banneradressen auf Übereinstimmung mit Masken aus den Listen für erlaubte und verbotene Adressen, falls diese Listen verwendet werden.

Gehen Sie folgendermaßen vor, um festzulegen, mit welchen Methoden Anti-Banner Adressen untersuchen soll:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Banner**.
3. Aktivieren Sie auf der rechten Fensterseite in der Gruppe **Untersuchungsmethoden** die Kontrollkästchen der zu verwendenden Methoden.

LISTEN FÜR VERBOTENE UND ERLAUBTE BANNERADRESSEN ERSTELLEN

Mit Hilfe von Listen für verbotene und erlaubte Banneradressen können Sie festlegen, von welchen Adressen das Laden und die Anzeige von Bannern verboten bzw. erlaubt werden soll. Anti-Banner blockiert den Download und die Anzeige der Banner von Adressen, die den Masken entsprechen, die auf der von Ihnen angelegten Schwarzen Liste stehen. Anti-Banner erlaubt den Download und die Anzeige der Banner von Adressen, die den Masken entsprechen, die auf der von Ihnen angelegten Weißen Liste stehen.

Gehen Sie folgendermaßen vor, um eine Maske zur Liste der verbotenen oder erlaubten Adressen hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Banner**.
3. Aktivieren Sie auf der rechten Fensterseite im Block **Erweitert** das Kontrollkästchen **Liste der verbotenen Webadressen verwenden** (oder **Liste der erlaubten Webadressen verwenden**) und klicken Sie unter dem Kontrollkästchen auf **Einstellungen**.

   Das Fenster **Verbotene Adressen** (oder **Erlaubte Adressen**) wird geöffnet.
4. Klicken Sie auf **Hinzufügen**.

   Das Fenster **Adressmaske (URL**) wird geöffnet.
5. Geben Sie die Maske einer verbotenen (oder erlaubten) Banneradresse ein und klicken Sie auf **OK**.

Damit eine bestimmte Maske nicht mehr verwendet wird, muss sie nicht gelöscht werden. Es ist ausreichend, im Fenster mit der Liste das entsprechende Kontrollkästchen zu deaktivieren.

ADRESSENLISTEN EXPORTIEREN / IMPORTIEREN

Listen für verbotene und erlaubte Banneradressen können mehrfach eingesetzt werden. Banneradressen können beispielsweise in eine entsprechende Liste auf einem anderen Computer übertragen werden, auf dem Kaspersky Internet Security installiert ist.

Dabei gilt folgendes Vorgehen:

1. *Exportieren* Sie eine Liste, d.h. die Einträge werden aus einer Liste in eine Datei kopiert.
2. Übertragen Sie die gespeicherte Datei auf einen anderen Computer (z.B. per E-Mail oder mit einem Wechseldatenträger).

3. *Importieren* Sie eine Liste, d.h. die Einträge werden aus einer Datei in eine analoge Liste auf einem anderen Computer eingetragen.

Beim Export einer Liste können Sie wählen, ob nur ausgewählte Listenelemente oder die gesamte Liste kopiert werden soll. Beim Import können der Liste neue Elemente hinzugefügt oder die vorhandene Liste durch eine importierte ersetzt werden.

Gehen Sie folgendermaßen vor, um Banneradressen aus der Liste für erlaubte oder verbotene Banneradressen zu exportieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Banner**.
3. Klicken Sie auf der rechten Fensterseite im Block **Erweitert** in der Zeile mit dem Namen der Liste, aus der Adressen in eine Datei kopiert werden sollen, auf **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster **Erlaubte Adressen** (oder im Fenster **Verbotene Adressen**) die Kontrollkästchen der Adressen, die in die Datei aufgenommen werden sollen.
5. Klicken Sie auf **Export**.

   Im folgenden Fenster können Sie wählen, welche Elemente exportiert werden sollen. Führen Sie hier eine der folgenden Aktionen aus:

   - Klicken Sie auf **Ja**, wenn nur ausgewählte Adressen in die Datei aufgenommen werden sollen.
   - Klicken Sie auf **Nein**, wenn die gesamte Liste in die Datei aufgenommen werden soll.
6. Geben Sie im folgenden Fenster einen Namen für die zu speichernde Datei ein und bestätigen Sie das Speichern.

Gehen Sie folgendermaßen vor, um Banneradressen aus einer Datei in eine Liste für erlaubte oder verbotene Adressen zu importieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Banner**.
3. Klicken Sie auf der rechten Fensterseite im Block **Erweitert** in der Zeile mit dem Namen der Liste, zu der Adressen aus einer Datei hinzugefügt werden sollen, auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster **Erlaubte Adressen** (oder im Fenster **Verbotene Adressen**) auf **Import**.

   Wenn die Liste nicht leer ist, wird Ihnen im folgenden Fenster vorgeschlagen, die zu importierenden Elemente hinzuzufügen. Führen Sie hier eine der folgenden Aktionen aus:

   - Klicken Sie auf **Ja**, wenn die Dateieinträge zur Liste hinzugefügt werden sollen.
   - Klicken Sie auf **Nein**, wenn die vorhandenen Einträge durch die Liste aus der Datei ersetzt werden sollen.
5. Wählen Sie im folgenden Fenster eine Datei mit den zu importierenden Einträgen.

SICHERE UMGEBUNG

Die Sichere Umgebung ist eine sichere, vom Betriebssystem isolierte Umgebung. Sie dient zum Start von Programmen, an deren Sicherheit Sie zweifeln, und zur Arbeit mit Online-Banking-Webseiten, bei denen die sichere Eingabe vertraulicher Daten besondere Bedeutung besitzt. Bei der Arbeit in der Sicheren Umgebung werden Objekte, die tatsächlich zum Betriebssystem gehören, nicht verändert. Selbst wenn Sie in der Sicheren Umgebung ein infiziertes Programm starten, bleiben seine Aktionen auf die virtuelle Umgebung beschränkt und haben keinen Einfluss auf das Betriebssystem.

In der aktuellen Version von Kaspersky Internet Security bietet die Sichere Umgebung folgende Optionen:

- Sicherer Programmstart (s. Abschnitt "Arbeit auf dem sicheren Desktop starten und beenden" auf S. 165).
- Bestimmtes Programm in sicherer Umgebung starten (auf S. 165).
- Sicherer Browser (auf S. 168).
- Virtuelle Tastatur (auf S. 68).

Verdächtige Objekte, die bei der Arbeit in der sicheren Umgebung gefunden werden, werden im normalen Modus in die Quarantäne verschoben. In der Liste der erkannten Bedrohungen und im vollständigen Bericht von Kaspersky Internet Security werden der Typ der Sicheren Umgebung und der Ursprungsort von Dateien gespeichert. Bei einer Wiederherstellung von Objekten aus der Quarantäne werden die Objekte im ursprünglichen Ordner wiederhergestellt. Wenn ein Ursprungsordner nicht gefunden werden kann, bietet Kaspersky Internet Security an, einen Wiederherstellungsort anzugeben, der sich in jener Umgebung befindet, in der der Wiederherstellungsvorgang gestartet wurde.

Auf Computern mit dem Betriebssystem Microsoft Windows XP x64 ist die Sichere Umgebung nicht verfügbar.

Auf Computern, die von Microsoft Windows XP x64 und Microsoft Windows 7 x64 verwaltet werden, kann die Funktionalität bestimmter Programme bei der Arbeit in der Sicheren Umgebung eingeschränkt sein. Beim Start solcher Programme erscheint eine entsprechende Meldung auf dem Bildschirm, wenn die Meldungen über das Ereignis **Die Funktionalität des Programms in der Sicheren Umgebung ist eingeschränkt** aktiviert wurden. Außerdem steht der sichere Desktop für den Start von Programmen nicht zur Verfügung.

IN DIESEM ABSCHNITT

Sicherer Programmstart 164

Sicherer Browser 168

SICHERER PROGRAMMSTART

Die Sichere Umgebung sollte für den Start von Programmen verwendet werden, an deren Sicherheit Sie zweifeln, sowie für vertrauenswürdige Programme, deren Schwachstellen von Angreifen benutzt werden können, um auf die Daten Ihres Computers zuzugreifen.

Sie können ein bestimmtes Programm in der sicheren Umgebung starten (s. Abschnitt "Bestimmtes Programm in sicherer Umgebung starten" auf S. 165) oder den sicheren Desktop verwenden (s. Abschnitt "Arbeit auf dem sicheren Desktop starten und beenden" auf S. 165).

Der sichere Desktop wird im Vollbildmodus geöffnet und stellt eine Kopie des normalen Desktops mit allen Objekten des Dateisystems dar.

Sie können eine Liste mit Programmen anlegen, die beim Start des sicheren Desktops automatisch gestartet werden sollen.

Wenn der Sichere Browser abgeschlossen wird, werden in der Grundeinstellung alle Veränderungen gespeichert, die während der Arbeit erfolgten, und sind beim folgenden Start wieder verfügbar. Bei Bedarf können Sie alle Veränderungen der sicheren Umgebung bereinigen (s. S. 168).

IN DIESEM ABSCHNITT

Bestimmtes Programm in Sicherer Umgebung starten 165

Arbeit auf dem sicheren Desktop starten und beenden 165

Zwischen normalem Desktop und Sicherer Umgebung wechseln 166

Popup-Symbolleiste verwenden 166

Automatischer Start von Programmen 167

Gemeinsamen Ordner verwenden 167

Sichere Umgebung für Programme bereinigen 168

BESTIMMTES PROGRAMM IN SICHERER UMGEBUNG STARTEN

Sie können einzelne Programme in der Sicheren Umgebung starten, ohne auf den sicheren Desktop umzuschalten. Der Start eines einzelnen Programms in der Sicheren Umgebung erfolgt aus dem Kontextmenü von Microsoft Windows;

Für Programme, die in der sicheren Umgebung gestartet wurden, besitzt das Programmfenster einen grünen Rahmen. Außerdem besitzen die Programme in der Liste der Programme, die von Programmkontrolle kontrolliert werden (s. Abschnitt "Programmkontrolle" auf S. 123), ein Merkmal für den sicheren Start.

Nachdem die Arbeit eines Programms abgeschlossen wurde, werden automatisch alle Veränderungen gelöscht, die im Verlauf der Programmarbeit erfolgt sind.

Um aus dem Kontextmenü von Microsoft Windows ein Programm in der Sicheren Umgebung zu starten,

öffnen Sie mit der rechten Maustaste das Kontextmenü für das gewählte Objekt (Verknüpfung oder ausführbare Programmdatei) und wählen Sie den Punkt **In Sicherer Umgebung starten**.

ARBEIT AUF DEM SICHEREN DESKTOP STARTEN UND BEENDEN

Der sichere Desktop kann auf folgende Arten gestartet werden:

- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47).
- aus dem Kontextmenü von Kaspersky Internet Security (s. Abschnitt "Kontextmenü" auf S. 46).
- mit Hilfe der entsprechenden Schaltfläche im Interface von Kaspersky Gadget, wenn für diese die Funktion zum Start des sicheren Desktops festgelegt ist (s. Abschnitt "Wie wird das Kaspersky Gadget verwendet?" auf S. 78).

Die Arbeit auf dem sicheren Desktop kann über das **Startmenü** des Betriebssystems, aus der Pop-up-Symbolleiste (s. Abschnitt "Pop-up-Symbolleiste verwenden" auf S. 166), oder mit der Tastenkombination **STRG+ALT+UMSCHALT+K** beendet werden.

Gehen Sie folgendermaßen vor, um den sicheren Desktop aus dem Hauptfenster von Kaspersky Internet Security zu starten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Sichere Umgebung** aus.
2. Wählen Sie auf der rechten Fensterseite **Sicherer Programmstart**.

- *Um den sicheren Desktop aus dem Kontextmenü von Kaspersky Internet Security zu starten,*

  klicken Sie mit der rechten Maustaste im Infobereich der Taskleiste auf das Symbol von Kaspersky Internet Security , um das Kontextmenü zu öffnen, und wählen Sie dort den Punkt **Sicherer Programmstart**.

- *Um den sicheren Desktop aus Kaspersky Gadget zu starten,*

  klicken Sie im Interface von Kaspersky Gadget auf die Schaltfläche mit dem Symbol **Sicherer Desktop** (nur für die Betriebssysteme Microsoft Windows Vista und Microsoft Windows 7).

- *Um die Arbeit in der Sicheren Umgebung aus dem Startmenü zu beenden,*

  gehen Sie im **Startmenü** des Betriebssystems den Punkt **Sicherer Programmstart – Beenden**.

- *Gehen Sie folgendermaßen vor, um die Arbeit in der Sicheren Umgebung aus der Popup-Symbolleiste zu beenden,*

  1. Zeigen Sie mit der Maus auf den oberen Bildschirmbereich.
  2. Klicken Sie in der Popup-Symbolleiste auf die Schaltfläche .
  3. Wählen Sie im folgenden Fenster zur Auswahl der Aktion den Punkt **Deaktivieren**.

ZWISCHEN NORMALEM DESKTOP UND SICHERER UMGEBUNG WECHSELN

Sie können zum normalen Desktop wechseln, ohne die Arbeit in der Sicheren Umgebung zu beenden, und anschließend erneut zur Sicheren Umgebung umschalten. Ein Wechsel zwischen dem sicheren und normalen Desktop ist auf folgende Weise möglich:

- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47).
- aus dem Kontextmenü von Kaspersky Internet Security (s. Abschnitt "Kontextmenü" auf S. 46).
- aus der Pop-up-Symbolleiste (s. Abschnitt "Pop-up-Symbolleiste verwenden" auf S. 166 - nur in der sicheren Umgebung verfügbar).
- mit Hilfe des Gadgets (s. Abschnitt "Kaspersky Gadget" auf S. 53).

- *Gehen Sie folgendermaßen vor, um aus dem Hauptfenster von Kaspersky Internet Security zum normalen Desktop zu wechseln:*

  1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Sichere Umgebung** aus.
  2. Wählen Sie auf der rechten Fensterseite **Normaler Desktop** aus.

- *Um aus dem Kontextmenü von Kaspersky Internet Security zum normalen Desktop zu wechseln,*

  klicken Sie mit der rechten Maustaste im Infobereich der Taskleiste auf das Symbol von Kaspersky Internet Security, um das Kontextmenü zu öffnen, und wählen Sie dort den Punkt **Normal**.

- *Gehen Sie folgendermaßen vor, um aus der Popup-Symbolleiste zum normalen Desktop zu wechseln:*

  1. Zeigen Sie mit der Maus auf den oberen Bildschirmbereich.
  2. Klicken Sie in der Popup-Symbolleiste auf die Schaltfläche .

POPUP-SYMBOLLEISTE VERWENDEN

Mit der Popup-Symbolleiste des sicheren Desktops können folgende Aktionen ausgeführt werden:

- Arbeit auf dem sicheren Desktop beenden (s. Abschnitt "Arbeit auf dem sicheren Desktop starten und beenden" auf S. 165).

- Wechsel zum normalen Desktop (s. Abschnitt "Zwischen normalem Desktop und sicherer Umgebung wechseln" auf S. 166).

Um die Popup-Symbolleiste auf dem sicheren Desktop anzuzeigen,

zeigen Sie mit der Maus auf den oberen Bildschirmbereich.

Gehen Sie folgendermaßen vor, um die Popup-Symbolleiste zu fixieren:

1. Zeigen Sie mit der Maus auf den oberen Bildschirmbereich.

2. Klicken Sie in der Popup-Symbolleiste auf die Schaltfläche .

AUTOMATISCHER START VON PROGRAMMEN

Sie können eine Liste mit Programmen anlegen, die beim Start des sicheren Desktops automatisch gestartet werden sollen.

Die Einrichtung des Autostarts ist nur bei der Arbeit mit dem sicheren Desktop verfügbar.

Gehen Sie folgendermaßen vor, um eine Autostart-Liste für den sicheren Desktop zu erstellen:

1. Wählen Sie im **Startmenü** des Betriebssystems den Punkt **Programme** → **Autostart** → **Sicherer Programmstart**.

2. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie dort den Punkt **Öffnen**.

3. Kopieren Sie die Verknüpfungen der Programme, die beim Start des sicheren Desktops automatisch gestartet werden sollen, in den geöffneten Ordner.

GEMEINSAMEN ORDNER VERWENDEN

Der gemeinsame Ordner der Sicheren Umgebung dient zum Dateiaustausch zwischen dem Hauptbetriebssystem und der sicheren Umgebung. Alle Dateien, die bei der Arbeit in der Sicheren Umgebung in diesem Ordner gespeichert werden, stehen vom normalen Desktop aus zur Verfügung.

Der gemeinsame Ordner wird bei der Programminstallation angelegt. Der Ort des gemeinsamen Ordners variiert in Abhängigkeit des Betriebssystems:

- für das Betriebssystem Microsoft Windows XP – C:\Dokumente und Einstellungen\All Users\Application Data\Kaspersky Lab\SandboxShared

- für die Betriebssysteme Microsoft Windows Vista und Microsoft Windows 7 – C:\ProgramData\Kaspersky Lab\SandboxShared

Der Ort des gemeinsamen Ordners kann nicht geändert werden.

Der gemeinsame Ordner der Sicheren Umgebung kann auf zwei Arten geöffnet werden:

- mit dem entsprechenden Link im Programmhauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 47);

- mit Hilfe der Verknüpfung, die durch das Symbol gekennzeichnet ist. Abhängig davon, welche Programmeinstellungen von den Entwicklern vorgegeben wurden, kann sich die Verknüpfung im Bereich "Arbeitsplatz" oder "Eigene Dokumente" des Explorers von Microsoft Windows befinden.

Gehen Sie folgendermaßen vor, um den gemeinsamen Ordner aus dem Hauptfenster von Kaspersky Internet Security zu öffnen:

1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Sichere Umgebung** aus.

2. Öffnen Sie auf der rechten Fensterseite im Block **Sicherer Programmstart** mit dem Link **Gemeinsamer Ordner** den gemeinsamen Ordner der Sicheren Umgebung (er wird in einem Standardfenster von Microsoft Windows geöffnet).

SICHERE UMGEBUNG FÜR PROGRAMME BEREINIGEN

Um die Daten zu löschen, die bei der Arbeit im Modus sicherer Programmstart gespeichert wurden, und geänderte Parameter wiederherzustellen, kann die Bereinigung der Sicheren Umgebung verwendet werden.

Die Bereinigung erfolgt auf dem normalen Desktop aus dem Hauptfenster von Kaspersky Internet Security und nur bei abgeschlossenem sicherem Programmstart.

Vergewissern Sie sich vor einer Bereinigung, dass alle Informationen, die künftig noch benötigt werden, im gemeinsamen Ordner der sicheren Umgebung gespeichert sind. Andernfalls werden die Daten gelöscht und können nicht wiederhergestellt werden.

Gehen Sie folgendermaßen vor, um die Daten der Sicheren Umgebung zu bereinigen:

1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Sichere Umgebung** aus.

2. Klicken Sie auf der rechten Fensterseite im Block **Sicherer Programmstart** auf den Link **Leeren**.

SICHERER BROWSER

Der Sichere Browser dient in erster Linie für den Zugriff auf Systeme für Online-Banking und sonstige Webseiten, die mit vertraulichen Daten arbeiten.

Sie können die Zugriffskontrolle für Online-Banking-Dienste aktivieren (s. Abschnitt "Zugriff auf Online-Banking-Dienste kontrollieren" auf S. 116), damit Bankseiten automatisch erkannt werden. Außerdem können Sie eine eigene Liste mit Webseiten anlegen, für die bei Zugriff vorgeschlagen werden soll, in den Sicheren Browsermodus zu wechseln.. Außerdem können Sie den Sicheren Browser manuell starten (s. Abschnitt "Sicheren Browser starten" auf S. 169).

Im Sicheren Browser verbleiben alle Änderungen (gespeicherte Cookies, Verlauf der besuchten Webseiten usw.) in der Sicheren Umgebung und gelangen nicht in das Betriebssystem. Deshalb können sie auch nicht von Angreifern verwendet werden. Bei Bedarf können Sie alle Veränderungen des Sicheren Browsers bereinigen und zu den ursprünglichen Einstellungen zurückkehren (s. Abschnitt "Browser nach Verwendung des Sicheren Browsers bereinigen" auf S. 169).

Bei der Arbeit in den Browsern Microsoft Internet Explorer, Mozilla Firefox und Google Chrome kann Kaspersky Internet Security automatisch erkennen, wenn zu unbekannten oder potentiell gefährlichen Webseiten gewechselt wird. Er kann dann vorschlagen, den Browser in der Sicheren Umgebung zu starten, um das Betriebssystem vor einem möglichen Risiko zu schützen, das mit dem Besuch unbekannter Webseiten verbunden ist.

Für die automatische Erkennung unbekannter Webseiten muss der Web-Filter (s. S. 115) von Web-Anti-Virus aktiviert sein.

IN DIESEM ABSCHNITT

Sicheren Browser starten 169

Browser nach Verwendung des Sicheren Browsers bereinigen 169

SICHEREN BROWSER STARTEN

Beim Start des Sicheren Browsers wird der standardmäßige Browser im sicheren Modus geöffnet (nur für Microsoft Internet Explorer, Mozilla Firefox und Google Chrome. In den übrigen Fällen wird im Sicheren Browser der Browser Microsoft Internet Explorer gestartet).

Wenn ein Browser im Sicheren Browsermodus läuft, ist sein Programmfenster grün eingerahmt.

Gehen Sie folgendermaßen vor, um den Sicheren Browser aus dem Hauptfenster von Kaspersky Internet Security zu starten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Sichere Umgebung**.
2. Wählen Sie auf der rechten Fensterseite **Sicherer Browser**.

BROWSER NACH VERWENDUNG DES SICHEREN BROWSERS BEREINIGEN

Um Daten, die bei der Arbeit gespeichert wurden, zu löschen, kann die Bereinigung des Sicheren Browsers verwendet werden.

Gehen Sie folgendermaßen vor, um die Daten des Sicheren Browsers zu bereinigen:

1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Sichere Umgebung** aus.
2. Klicken Sie auf der rechten Fensterseite im Block **Sicherer Browser** auf den Link **Leeren**.

KINDERSICHERUNG

Die *Kindersicherung* kann die Aktionen unterschiedlicher Benutzer auf einem Computer und im Netzwerk kontrollieren. Die Kontrolle umfasst hierbei einerseits die Möglichkeit, den Zugriff auf Ressourcen und Programme zu beschränken, andrerseits die Anzeige von Berichten über die Benutzeraktionen.

Die Zahl der Kinder und Jugendlichen, die Zugang zu Computern und zum Internet besitzen, nimmt kontinuierlich zu. Durch die Risiken, mit denen die Arbeit und Kommunikation im Internet verbunden sind, ergeben sich Sicherheitsprobleme. Die wichtigsten Probleme sind:

- Besuch von Webseiten, die Zeitverlust (Chats, Online-Spiele) oder Geldverlust (Internet-Shops, Auktionen) verursachen können.
- Zugriff auf Webressourcen, die für Erwachsene bestimmt sind (z.B. Seiten, die pornografische oder extremistische Materialien enthalten, die Themen wie Waffen, Drogen und Gewalt betreffen).
- Download von infizierten Dateien.
- unverhältnismäßig lange Arbeit am Computer und damit verbundene gesundheitliche Risiken.
- Kontakte mit Fremden, die sich als Gleichaltrige ausgeben und persönliche Informationen über den Benutzer erhalten können (z.B. echter Name, Adresse, Zeiten, zu denen Kinder unbeaufsichtigt zuhause sind).

Die Kindersicherung erlaubt es, die mit der Arbeit am Computer und im Internet verbundenen Risiken zu reduzieren. Dazu dienen folgende Funktionen des Moduls:

- zeitliche Beschränkung für die Verwendung von Computer und Internet.
- Erstellen von Listen für zum Start erlaubte und verbotene Programme, sowie vorübergehende Beschränkung des Starts von erlaubten Programmen.

- Erstellen von Listen mit Webseiten, auf die der Zugriff erlaubt bzw. verboten ist. Auswahl von inhaltlichen Kategorien für Webressourcen, die nicht zur Ansicht empfohlen sind.
- Aktivieren des Modus zur sicheren Suche mit Suchmaschinen (Links zu Webseiten mit verdächtigem Inhalt werden nicht in den Suchergebnissen angezeigt).
- Beschränkung des Downloads von Dateien aus dem Internet.
- Erstellen von Listen mit Kontakten, für die die Kommunikation über Instant Messenger und in sozialen Netzwerken erlaubt oder verboten wird.
- Kontrolle des Texts von Nachrichten, die mit Instant Messengern und in sozialen Netzwerken ausgetauscht werden.
- Sendeverbot von bestimmten persönlichen Daten.
- Suche nach bestimmten Schlüsselwörtern im Nachrichtentext.

Alle Beschränkungen können einzeln aktiviert werden, wodurch sich die Kindersicherung flexibel auf unterschiedliche Benutzer anpassen lässt. Für jedes Benutzerkonto können Berichte angezeigt werden, die Ereignisse der kontrollierten Kategorien für einen bestimmten Zeitraum umfassen.

Um die Komponente zu verwalten, ist eine Authentifizierung erforderlich: Geben Sie den Namen und das Kennwort des Administrators ein (s. Abschnitt "Kontrolle des Zugriffs auf Kaspersky Internet Security" auf S. 83). Sollten Sie noch kein Kennwort für die Verwaltung von Kaspersky Internet Security festgelegt haben, so wird Ihnen vorgeschlagen, dies zu tun.

IN DIESEM ABSCHNITT

Kindersicherung für einen Benutzer anpassen..... 170

Berichte über die Aktionen eines Benutzers anzeigen..... 179

KINDERSICHERUNG FÜR EINEN BENUTZER ANPASSEN

Sie können die Kindersicherung für jedes Benutzerkonto individuell aktivieren und anpassen. Dazu werden für die einzelnen Benutzer entsprechende Beschränkungen festlegen, die z.B. vom Alter abhängig sind. Für Benutzer, deren Aktionen nicht kontrolliert werden sollen, können Sie die Kindersicherung deaktivieren.

IN DIESEM ABSCHNITT

Benutzerkontrolle aktivieren und deaktivieren 171

Parameter der Kindersicherung exportieren / importieren 172

Darstellung eines Benutzerkontos in Kaspersky Internet Security 173

Arbeitszeit auf dem Computer 174

Start von Programmen 174

Arbeitszeit im Internet 174

Besuch von Webseiten 175

Download von Dateien aus dem Internet 175

Korrespondenz über Instant Messenger 176

Korrespondenz in sozialen Netzwerken 177

Senden vertraulicher Informationen 178

Suche nach Schlüsselwörtern 178

BENUTZERKONTROLLE AKTIVIEREN UND DEAKTIVIEREN

Sie können die Kindersicherung für jedes Benutzerkonto separat aktivieren und deaktivieren. Es ist beispielsweise überflüssig, die Aktionen eines erwachsenen Benutzers, der für den Computer über Administratorrechte verfügt, zu kontrollieren. Für ihn kann die Kindersicherung deaktiviert werden. Für die übrigen Benutzer, deren Aktionen kontrolliert werden soll, muss die Kindersicherung aktiviert und angepasst werden. Dazu können z.B. standardmäßige Einstellungen aus einer Vorlage geladen werden.

Die Kindersicherung kann auf folgende Arten für ein bestimmtes Benutzerkonto aktiviert und deaktiviert werden:

- aus dem Programmhauptfenster
- aus dem Fenster **Kindersicherung**
- aus dem Konfigurationsfenster der Kindersicherung

Die Aktivierung und Deaktivierung der Kindersicherung für das aktuelle Benutzerkonto kann aus dem Kontextmenü des Programmsymbols erfolgen.

Gehen Sie folgendermaßen vor, um die Kindersicherung für ein Benutzerkonto vom Hauptfenster aus zu aktivieren oder zu deaktivieren:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.

2. Klicken Sie auf der rechten Fensterseite im Block mit dem Benutzerkonto auf die Schaltfläche , um die Kindersicherung für das Benutzerkonto einzuschalten. Um die Kindersicherung auszuschalten, klicken Sie auf die Schaltfläche .

- *Gehen Sie folgendermaßen vor, um die Kindersicherung für ein Benutzerkonto vom Fenster der Kindersicherung aus zu aktivieren oder zu deaktivieren:*

  1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.

  2. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, für das die Kindersicherung aktiviert oder deaktiviert werden soll.

     Das Fenster **Kindersicherung** wird geöffnet

  3. Wählen Sie die Registerkarte **Einstellungen** und wählen Sie auf der linken Fensterseite den Abschnitt **Einstellungen für Benutzerkonto**.

  4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kindersicherung aktivieren**, um die Kindersicherung für das Benutzerkonto einzuschalten. Entfernen Sie das Kontrollkästchen, um die Kindersicherung für ein Benutzerkonto zu deaktivieren.

  5. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

- *Gehen Sie folgendermaßen vor, um die Kindersicherung für ein Benutzerkonto vom Programmkonfigurationsfenster aus zu aktivieren oder zu deaktivieren:*

  1. Öffnen Sie das Programmkonfigurationsfenster.

  2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Unterabschnitt **Kindersicherung**.

  3. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, für das die Kindersicherung aktiviert oder deaktiviert werden soll.

  4. Klicken Sie über der Benutzerliste auf **Kontrollieren**, um die Kindersicherung zu aktivieren. Um die Kindersicherung auszuschalten, klicken Sie auf **Deaktivieren**.

- *Gehen Sie folgendermaßen vor, um die Kindersicherung für das aktuelle Benutzerkonto aus dem Kontextmenü des Programmsymbols zu aktivieren oder zu deaktivieren:*

  1. Öffnen Sie durch Rechtsklick das Kontextmenü des Programmsymbols (s. Abschnitt "Kontextmenü" auf S. 46).

  2. Wählen Sie den Menüpunkt **Kindersicherung aktivieren** aus, um die Kindersicherung für das aktuelle Benutzerkonto zu aktivieren. Wählen Sie den Menüpunkt **Kindersicherung deaktivieren** aus, um die Kindersicherung für das aktuelle Benutzerkonto zu deaktivieren.

PARAMETER DER KINDERSICHERUNG EXPORTIEREN / IMPORTIEREN

Wenn Sie die Kindersicherung bereits für ein Benutzerkonto angepasst haben, können die Einstellungen in einer separaten Datei gespeichert werden (*Export* ausführen). Die Einstellungen können später aus dieser Datei geladen werden, um die Komponente schnell anzupassen (*Import* ausführen). Außerdem können die Parameter, die für die Kontrolle eines anderen Benutzerkontos gelten, übernommen oder es kann eine Konfigurationsvorlage verwendet werden (eine vordefinierte Auswahl von Regeln für unterschiedliche Benutzertypen, die sich an Alter, Erfahrung und anderen Merkmalen orientieren).

Nachdem eine Auswahl von Parametern für ein Benutzerkonto übernommen wurde, können die Werte geändert werden. Dies hat keinen Einfluss auf die Werte in der Datei, aus der die Einstellungen importiert wurden.

- *Gehen Sie folgendermaßen vor, um die Kontrollparameter in einer Datei zu speichern:*

  1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.

  2. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, dessen Kontrolleinstellungen gespeichert werden sollen.

3. Wählen Sie auf der linken Seite des folgenden Fensters den Abschnitt **Einstellungen des Benutzerkontos**.

4. Klicken Sie im unteren Bereich des Fensters auf **Speichern** und speichern Sie die Konfigurationsdatei.

Gehen Sie folgendermaßen vor, um Kontrollparameter aus einer Datei zu laden:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.

2. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, für das die Kontrolleinstellungen geladen werden sollen.

3. Wählen Sie auf der linken Seite des folgenden Fensters den Abschnitt **Einstellungen des Benutzerkontos**.

4. Klicken Sie im unteren Fensterbereich auf **Laden**.

5. Wählen Sie im folgenden Fenster **Einstellungen für Kindersicherung laden** die Variante **Konfigurationsdatei** und geben Sie den Pfad der Datei an.

Gehen Sie folgendermaßen vor, um die Parameter eines Benutzerkontos zu übernehmen:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.

2. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, für das die Kontrolleinstellungen geladen werden sollen.

3. Wählen Sie auf der linken Seite des folgenden Fensters den Abschnitt **Einstellungen des Benutzerkontos**.

4. Klicken Sie im unteren Fensterbereich auf **Laden**.

5. Wählen Sie im folgenden Fenster **Einstellungen für Kindersicherung laden** die Variante **Anderer Benutzer** und geben Sie das Benutzerkonto an, dessen Einstellungen verwendet werden sollen.

Gehen Sie folgendermaßen vor, um eine Konfigurationsvorlage zu verwenden:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.

2. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, für das die Kontrolleinstellungen aus einer Vorlage geladen werden sollen.

3. Wählen Sie auf der linken Seite des folgenden Fensters den Abschnitt **Einstellungen des Benutzerkontos**.

4. Klicken Sie im unteren Fensterbereich auf **Laden**.

5. Wählen Sie im folgenden Fenster **Einstellungen für Kindersicherung laden** die Variante **Vorlage** und geben Sie die Vorlage an, deren Einstellungen verwendet werden sollen.

DARSTELLUNG EINES BENUTZERKONTOS IN KASPERSKY INTERNET SECURITY

Sie können ein Alias und ein Bild wählen, die in Kaspersky Internet Security für ein Benutzerkonto angezeigt werden sollen.

Gehen Sie folgendermaßen vor, um ein Alias und ein Bild für ein Benutzerkonto festzulegen:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.

2. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, dessen Darstellung angepasst werden soll.

3. Wählen Sie auf der linken Seite des folgenden Fensters den Abschnitt **Einstellungen des Benutzerkontos**.
4. Geben Sie im Feld **Alias** ein Alias für den Benutzer an.
5. Wählen Sie ein Bild für das Benutzerkonto.
6. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

ARBEITSZEIT AUF DEM COMPUTER

Sie können einen Zeitplan einrichten, der den Zugriff eines Benutzers auf den Computer reguliert (Wochentage und Zeiträume im Verlauf eines Tages). Außerdem kann die tägliche Arbeitszeit auf dem Computer begrenzt werden.

Gehen Sie folgendermaßen vor, um die Verwendung des Computers zeitlich zu beschränken:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.
2. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll.
3. Wählen Sie auf der linken Seite des folgenden Fensters den Abschnitt **Verwendung des Computers**.
4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
5. Legen Sie die zeitlichen Beschränkungen für die Verwendung des Computers fest.
6. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

START VON PROGRAMMEN

Sie können den Start bestimmter Programme erlauben oder verbieten. Außerdem kann der Start erlaubter Programme zeitlich eingeschränkt werden.

Gehen Sie folgendermaßen vor, um den Start von Programmen einzuschränken:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.
2. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll.
3. Wählen Sie auf der linken Seite des folgenden Fensters den Abschnitt **Start von Programmen**.
4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
5. Erstellen Sie die Listen für Programme, deren Start erlaubt bzw. verboten ist, und legen Sie einen Zeitplan für die Verwendung von erlaubten Programmen fest.
6. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

ARBEITSZEIT IM INTERNET

Sie können die Zeit, die ein Benutzer im Internet verbringen darf, beschränken. Dazu lässt sich ein Zeitplan für den Internetzugriff einstellen (Wochentage und Zeiträume im Verlauf eines Tages, in denen der Zugriff erlaubt oder verboten ist). Außerdem kann die tägliche Verwendungsdauer für das Internet begrenzt werden.

Gehen Sie folgendermaßen vor, um die Verwendung des Internets zeitlich zu beschränken:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.

2. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll.
3. Wählen Sie auf der linken Seite des folgenden Fensters den Abschnitt **Verwendung des Internets**.
4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
5. Legen Sie die zeitlichen Beschränkungen für die Verwendung des Internets fest.
6. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

BESUCH VON WEBSEITEN

Sie können den Zugriff auf Webseiten in Abhängigkeit von ihrem Inhalt beschränken. Dazu können Kategorien von Webseiten gewählt werden, auf die der Zugriff blockiert werden soll. Außerdem kann eine Liste von Ausnahmen angelegt werden.

Sie können den *Modus für sichere Suche* aktivieren, der zum Einsatz kommt, wenn ein Benutzer mit Suchmaschinen arbeitet. Bestimmte Suchmaschinen versuchen, ihre Nutzer vor unzulässigen Inhalten auf Webressourcen zu schützen. Dazu werden Webseiten bei der Indizierung auf Schlüsselwörter und Phrasen, Adressen und Ressourcenkategorien hin analysiert. Wenn der Modus für sichere Suche aktiviert ist, werden Webseiten, die unerwünschten Kategorien angehören (Pornografie, Drogen, Gewalt und sonstige Materialien, die nicht für Minderjährige geeignet sind), von den Suchergebnissen ausgeschlossen.

Die Kindersicherung erlaubt es, den Modus für sichere Suche gleichzeitig für folgende Suchmaschinen zu aktivieren:

- Google
- Bing.com

Gehen Sie folgendermaßen vor, um den Zugriff auf Webseiten zu beschränken:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.
2. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll.
3. Wählen Sie auf der linken Seite des folgenden Fensters den Abschnitt **Besuch von Webseiten**.
4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
5. Wählen Sie Kategorien von Webseiten, auf die der Zugriff blockiert werden soll.
6. Um den Zugriff auf bestimmte Webseiten, die eigentlich zu einer verbotenen Kategorie gehören, zu erlauben, oder den Zugriff auf Seiten, die nicht zu einer Verbotskategorie gehören, zu verbieten, fügen Sie sie zur Ausnahmeliste hinzu. Klicken Sie dazu auf **Ausnahmen**, um das Fenster **Webseiten verbieten: Ausnahmen** zu öffnen.
7. Aktivieren Sie das Kontrollkästchen **Modus für sichere Suche aktivieren**, um den sicheren Suchmodus zu aktivieren.
8. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

DOWNLOAD VON DATEIEN AUS DEM INTERNET

Sie können festlegen, welche Dateitypen ein Benutzer aus dem Internet herunterladen darf.

Gehen Sie folgendermaßen vor, um den Download von Dateien aus dem Internet einzuschränken:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.

2. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll.
3. Wählen Sie auf der linken Seite des folgenden Fensters den Abschnitt **Download von Dateien**.
4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
5. Wählen Sie die Dateikategorien, deren Download erlaubt ist.
6. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

KORRESPONDENZ ÜBER INSTANT MESSENGER

Die Kontrolle der Korrespondenz mit Programmen zum Nachrichtensofortversand (Instant Messenger) umfasst die Kontrolle von erlaubten Kontakten, das Blockieren der Korrespondenz mit verbotenen Kontakten, sowie die Kontrolle des Nachrichteninhalts. Sie können Listen mit erlaubten und verbotenen Kontakten anlegen, Schlüsselwörter festlegen, auf deren Vorhandensein die Nachrichten überprüft werden, und persönliche Informationen, die nicht gesendet werden dürfen, angeben.

Wenn die Korrespondenz mit einem Kontakt verboten ist, werden alle Nachrichten, die sich an diesen Kontakt richten oder von ihm stammen, blockiert. Informationen über blockierte Nachrichten und das Vorhandensein von Schlüsselwörtern in Nachrichten werden protokolliert. Im Bericht sind auch die Nachrichtentexte für jeden Kontakt enthalten.

Die Korrespondenz-Kontrolle besitzt folgende Einschränkungen:

- Wenn ein Instant Messenger gestartet wurde, bevor die Kindersicherung aktiviert wurde, erfolgt die Korrespondenz-Kontrolle erst nach einem Neustart des Instant Messengers.
- Bei Verwendung eines HTTP-Proxys wird die Korrespondenz nicht kontrolliert.

Die aktuelle Version der Kindersicherung bietet die Kontrolle für folgende Instant Messenger:

- ICQ
- QIP
- Windows Live Messenger (MSN)
- Yahoo Messenger
- GoogleTalk
- mIRC
- Mail.Ru Agent
- Psi
- Miranda
- AIM
- Digsby
- Pidgin
- Qnext
- SIM
- Trilian

- Xchat
- Instantbird
- RnQ
- MSN
- Jabber

Manche Instant Messenger wie z.B. Yahoo! Messenger und Google Talk verwenden eine geschützte Verbindung. Um den Datenverkehr dieser Programme zu untersuchen, muss die Untersuchung von geschützten Verbindungen aktiviert werden (s. S. 139).

Gehen Sie folgendermaßen vor, um die Kontakte, für die die Korrespondenz mit Instant Messengern möglich ist, zu beschränken:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.
2. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll.
3. Wählen Sie auf der linken Seite des folgenden Fensters den Abschnitt **IM-Korrespondenz**.
4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
5. Legen Sie die Listen für erlaubte und verbotene Kontakte an.
6. Geben Sie eine Standardaktion für Kontakte an, die nicht zur Liste gehören: Soll die Kommunikation mit solchen Kontakten verboten werden, so aktivieren Sie das Kontrollkästchen **Kommunikation mit anderen Kontakten verbieten**. Deaktivieren Sie das Kontrollkästchen, um die Kommunikation mit Kontakten zu erlauben, die nicht zur Liste gehören.
7. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

KORRESPONDENZ IN SOZIALEN NETZWERKEN

Die Kontrolle der Korrespondenz über soziale Netzwerke umfasst die Kontrolle von erlaubten Kontakten, das Blockieren der Korrespondenz mit verbotenen Kontakten, sowie die Kontrolle des Nachrichteninhalts. Sie können Listen mit erlaubten und verbotenen Kontakten anlegen, Schlüsselwörter festlegen, auf deren Vorhandensein die Nachrichten überprüft werden, und persönliche Informationen, die nicht gesendet werden dürfen, angeben.

Wenn die Korrespondenz mit einem Kontakt verboten ist, werden alle Nachrichten, die sich an diesen Kontakt richten oder von ihm stammen, blockiert. Informationen über blockierte Nachrichten und das Vorhandensein von Schlüsselwörtern in Nachrichten werden protokolliert. Im Bericht sind auch die Nachrichtentexte für jeden Kontakt enthalten.

Manche sozialen Netzwerke wie z.B. Twitter verwenden eine geschützte Verbindung. Um den Datenverkehr dieser Netzwerke zu untersuchen, muss die Untersuchung von geschützten Verbindungen aktiviert werden (s. S. 139).

Gehen Sie folgendermaßen vor, um die Kontakte, für die die Korrespondenz über soziale Netzwerke möglich ist, zu beschränken:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.
2. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll.
3. Wählen Sie auf der linken Seite des folgenden Fensters den Abschnitt **Soziale Netzwerke**.

4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.

5. Geben Sie eine Standardaktion für Kontakte an, die nicht zur Liste der kontrollierten Kontakte gehören: Soll die Kommunikation mit solchen Kontakten verboten werden, so aktivieren Sie das Kontrollkästchen **Kommunikation mit anderen Kontakten verbieten**. Deaktivieren Sie das Kontrollkästchen, um die Kommunikation mit Kontakten zu erlauben, die nicht zur Liste der kontrollierten Kontakte gehören.

6. Wählen Sie die Registerkarte **Berichte**.

7. Wählen Sie auf der linken Fensterseite den Abschnitt **Soziale Netzwerke**.

   Auf der rechten Fensterseite befindet sich eine Liste der Kontakte, von denen eine Nachricht empfangen oder an die eine Nachricht gesendet wurde.

8. Geben Sie eine Aktion für die gewählten Kontakte an (Korrespondenz verbieten oder erlauben).

   Die Kontakte werden automatisch zur Liste der kontrollierten Kontakte hinzugefügt, die auf der Registerkarte **Einstellungen** im Abschnitt **Soziale Netzwerke** angezeigt wird.

9. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

SENDEN VERTRAULICHER INFORMATIONEN

Sie können verbieten, dass Daten, die persönliche Informationen enthalten, über Instant Messenger, soziale Netzwerke und beim Senden von Daten über Webseiten verschickt werden. Dafür ist es erforderlich, eine Liste mit Einträgen anzulegen, die vertrauliche Informationen enthalten (z.B. Adresse, Telefonnummer usw.).

Versuche zum Senden von Daten aus dieser Liste werden blockiert, und es werden Informationen über blockierte Nachrichten im Bericht aufgezeichnet.

Gehen Sie folgendermaßen vor, um das Senden von persönlichen Daten zu blockieren:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.

2. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll.

3. Wählen Sie auf der linken Seite des folgenden Fensters den Abschnitt **Persönliche Daten**.

4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.

5. Legen Sie eine Liste mit persönlichen Daten an, die nicht gesendet werden dürfen.

6. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

SUCHE NACH SCHLÜSSELWÖRTERN

Sie können kontrollieren, ob in der Korrespondenz eines Benutzers, die über Instant Messenger, soziale Netzwerke und beim Senden von Daten über Webseiten erfolgt, bestimmte Wörter oder Phrasen vorkommen.

Das Vorhandensein von festgelegten Schlüsselwörtern in ausgetauschten Nachrichten wird protokolliert.

Wenn die Korrespondenz-Kontrolle für Instant Messenger und soziale Netzwerke oder die Kontrolle für den Besuch von Webseiten deaktiviert ist, erfolgt keine Suche nach Schlüsselwörtern.

Gehen Sie folgendermaßen vor, um zu kontrollieren, ob in der Korrespondenz und in gesendeten Daten bestimmte Wörter vorkommen:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.
2. Wählen Sie auf der rechten Fensterseite ein Benutzerkonto, für das eine Beschränkung festgelegt werden soll.
3. Wählen Sie auf der linken Seite des folgenden Fensters den Abschnitt **Schlüsselwörter**.
4. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
5. Legen Sie eine Liste mit Schlüsselwörtern an, auf die die Korrespondenz und die gesendeten Daten kontrolliert werden sollen.
6. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

BERICHTE ÜBER DIE AKTIONEN EINES BENUTZERS ANZEIGEN

Sie können Berichte über die Aktionen jedes Benutzers ansehen, für den die Kindersicherung aktiviert wurde. Es sind Berichte für jede Kategorie der kontrollierten Ereignisse verfügbar.

Gehen Sie folgendermaßen vor, um einen Bericht über die Aktionen eines kontrollierten Benutzers anzuzeigen:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Kindersicherung**.
2. Wählen Sie auf der rechten Fensterseite den Block für das Benutzerkonto, über dessen Aktionen ein Bericht angezeigt werden soll.
3. Wählen Sie die Registerkarte **Berichte**.
4. Wählen Sie auf der linken Fensterseite die Kategorie der kontrollierten Aktionen oder des Inhalts (z.B. **Verwendung des Internet** der **Persönliche Daten**).

   Auf der rechten Fensterseite befindet sich ein Bericht über die kontrollierten Aktionen und Inhalte.

VERTRAUENSWÜRDIGE ZONE

Die *vertrauenswürdige Zone* ist eine benutzerdefinierte Liste von Objekten, die nicht von dem Programm kontrolliert werden. Mit anderen Worten ist dies eine Auswahl von Ausnahmen für den Schutz, den Kaspersky Internet Security bietet.

Die vertrauenswürdige Zone wird auf Basis einer Liste der vertrauenswürdigen Programme (s. Abschnitt "Liste mit vertrauenswürdigen Programmen erstellen" auf S. 180) und der Ausnahmeregeln (s. Abschnitt "Ausnahmeregeln erstellen" auf S. 181) eingerichtet, wobei die Besonderheiten der Objekte, mit denen Sie arbeiten, sowie der Programme, die auf Ihrem Computer installiert sind, zu berücksichtigen sind. Die Aufnahme von Objekten in die vertrauenswürdige Zone kann beispielsweise erforderlich sein, wenn Kaspersky Internet Security den Zugriff auf ein bestimmtes Objekt oder Programm blockiert, Sie aber sicher sind, dass dieses Objekt / Programm absolut unschädlich ist.

Wenn Sie beispielsweise die Objekte, die von dem standardmäßigen Windows-Editor verwendet werden, für ungefährlich und ihre Untersuchung für nicht erforderlich halten, Sie diesem Programm also vertrauen, dann fügen Sie den Editor zur Liste der vertrauenswürdigen Programme hinzu, um die Objekte, die von diesem Prozess benutzt werden, von der Untersuchung auszuschließen.

Außerdem können bestimmte Aktionen, die als gefährlich klassifiziert werden, im Rahmen der Funktionalität bestimmter Programme ungefährlich sein. So ist das Abfangen eines über die Tastatur eingegebenen Texts für Programme zum automatischen Umschalten der Tastaturbelegung (z.B. Punto Switcher) eine normale Aktion. Um die Besonderheit solcher Programme zu berücksichtigen und die Kontrolle ihrer Aktivität abzuschalten, empfehlen wir, sie in die Liste der vertrauenswürdigen Anwendungen aufzunehmen.

Wenn ein Programm der vertrauenswürdigen Liste hinzugefügt wird, werden die Datei- und Netzwerkaktivität dieses Programms (einschließlich verdächtiger Aktivität) sowie seine Zugriffe auf die Systemregistrierung nicht kontrolliert. Zugleich werden die ausführbare Datei und der Prozess eines vertrauenswürdigen Programms weiterhin auf Viren untersucht. Um ein Programm vollständig von der Untersuchung auszuschließen, müssen die Ausnahmeregeln verwendet werden.

Durch das Ausschließen vertrauenswürdiger Programme von der Untersuchung lassen sich Kompatibilitätsprobleme von Kaspersky Internet Security mit anderen Programmen vermeiden (beispielsweise Probleme einer doppelten Untersuchung des Netzwerkverkehrs eines anderen Computers durch Kaspersky Internet Security und durch ein anderes Antiviren-Programm). Außerdem lässt sich dadurch die Leistungsfähigkeit des Computers erhöhen, was speziell bei der Verwendung von Serverprogrammen wichtig ist.

Die Ausnahmeregeln der vertrauenswürdigen Zone gewährleisten ihrerseits die Möglichkeit, mit legalen Programmen zu arbeiten, die von Angreifern für die Schädigung des Computers oder der Daten des Benutzers verwendet werden können. Solche Programme haben zwar selbst keine schädlichen Funktionen, können aber von Schadprogrammen als Hilfskomponenten missbrauch werden. Zu dieser Kategorie gehören beispielsweise Programme zur Remote-Verwaltung, IRC-Clients, FTP-Server, unterschiedliche Hilfsprogramme zum Beenden von Prozessen und zum Verstecken ihrer Arbeit, Tastaturspione, Programme zur Kennwortermittlung, Programme zur automatischen Einwahl auf kostenpflichtige Webseiten u.a. Derartige Programme können aufgrund der Arbeit von Kaspersky Internet Security gesperrt werden. Um das Sperren zu verhindern, können für die verwendeten Programme Ausnahmeregeln erstellt werden.

Eine *Ausnahmeregel* ist eine Kombination von Bedingungen, bei deren Erfüllung ein Objekt nicht von Kaspersky Internet Security untersucht wird. In allen übrigen Fällen wird dieses Objekt von allen Schutzkomponenten mit den festgelegten Parametern untersucht.

Die Ausnahmeregeln der vertrauenswürdigen Zone können von mehreren Programmkomponenten (z.B. Datei-Anti-Virus, Mail-Anti-Virus, Web-Anti-Virus (s. Abschnitt "Web-Anti-Virus" auf S. 108)) sowie bei der Ausführung von Untersuchungsaufgaben verwendet werden.

IN DIESEM ABSCHNITT

Liste mit vertrauenswürdigen Programmen erstellen 180

Ausnahmeregeln erstellen..... 181

LISTE MIT VERTRAUENSWÜRDIGEN PROGRAMMEN ERSTELLEN

Kaspersky Internet Security untersucht standardmäßig alle Objekte, die von einem beliebigen Programmprozess geöffnet, gestartet oder gespeichert werden sollen, und kontrolliert die Aktivität aller Programme und den von ihnen erzeugten Netzwerkverkehr. Die Programme der vertrauenswürdigen Liste werden von Kaspersky Internet Security von der Untersuchung ausgeschlossen.

Gehen Sie folgendermaßen vor, um ein Programm zur Liste der vertrauenswürdigen Programme hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Bedrohungen und Ausnahmen**.
3. Klicken Sie im Block **Ausnahmen** auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Vertrauenswürdige Programme** auf die Schaltfläche **Hinzufügen**, um das Menü zur Programmauswahl zu öffnen.
5. Wählen Sie ein Programm aus der Dropdown-Liste **Programme** oder gehen Sie auf den Punkt **Durchsuchen**, um den Pfad der ausführbaren Datei des entsprechenden Programms anzugeben.
6. Aktivieren Sie im folgenden Fenster **Ausnahmen für das Programm** die Kontrollkästchen für die Arten der Programmaktivität, die nicht untersucht werden sollen.

Mit Hilfe der entsprechenden Schaltflächen im oberen Bereich der Liste können Sie ein vertrauenswürdiges Programm ändern oder es aus der Liste löschen. Um ein Programm aus der Liste auszuschließen, ohne es zu entfernen, deaktivieren Sie das entsprechende Kontrollkästchen.

AUSNAHMEREGELN ERSTELLEN

Falls Sie in Ihrer Arbeit Programme benutzen, die von Kaspersky Internet Security als illegal eingestuft werden und von Angreifen zur Schädigung des Computers oder der Daten des Benutzers verwendet werden können, empfehlen wir Ihnen, für diese Ausnahmen einzurichten.

Gehen Sie folgendermaßen vor, um eine Ausnahmeregel zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Bedrohungen und Ausnahmen**.
3. Klicken Sie im Block **Ausnahmen** auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Regeln für Ausnahmen** auf **Hinzufügen**.
5. Geben Sie im folgenden Fenster **Ausnahmeregel** die Parameter der Ausnahmeregel an.

LEISTUNG UND KOMPATIBILITÄT MIT ANDEREN PROGRAMMEN

Die Leistungseinstellungen für Kaspersky Internet Security umfassen das Spektrum der erkennbaren Bedrohungen sowie Energieverbrauch und benötigte Computerressourcen.

Kaspersky Internet Security erlaubt es, das Schutzspektrum flexibel anzupassen und unterschiedliche Bedrohungskategorien (s. Abschnitt "Kategorien der erkennbaren Bedrohungen wählen" auf S. 182) zu wählen, die das Programm bei der Arbeit erkennen soll.

Bei der Arbeit auf einem Laptop besitzt der Energieverbrauch, der von Programmen verursacht wird, eine besondere Bedeutung. Eine Virenuntersuchung des Computers und das Datenbank-Update beanspruchen erhebliche Ressourcen. Ein spezieller Modus für die Arbeit von Kaspersky Internet Security auf einem Laptop (s. S. 184) schiebt geplante Untersuchungs- und Updateaufgaben automatisch auf, wenn die Stromversorgung von einer Batterie erfolgt, und spart dadurch Akkustrom. Der Modus zur Untersuchung im Computerleerlauf (s. Abschnitt "Aufgabenstart im Hintergrundmodus" auf S. 183) erlaubt es, ressourcenaufwändige Aufgaben dann zu starten, wenn der Computer nicht verwendet wird.

Der von Kaspersky Internet Security verursachte Verbrauch von Computerressourcen kann sich auf die Performance anderer Programme auswirken. Um bei der gleichzeitigen Arbeit mit anderen Programmen Probleme durch eine hohe Last auf Prozessor und Laufwerk-Subsysteme zu vermeiden, kann Kaspersky Internet Security Untersuchungsaufgaben anhalten und Ressourcen für andere Programme freigeben (s. S. 183), die auf dem Computer laufen.

Im Modus Profil für Spiele wird die Anzeige von Meldungen über die Arbeit von Kaspersky Internet Security automatisch deaktiviert, wenn andere Programme im Vollbildmodus gestartet werden.

Der erweiterte Desinfektionsvorgang, der für den Fall einer aktiven Infektion vorgesehen ist, erfordert einen obligatorischen Neustart des Computers, was sich ebenfalls auf die Arbeit anderer Programme auswirken kann. Bei Bedarf können Sie die Verwendung der Technologie zur Desinfektion aktiver Infektionen (s. S. 182) deaktivieren, um eine unerwünscht hohe Auslastung des Computers zu vermeiden.

IN DIESEM ABSCHNITT

Kategorien der erkennbaren Bedrohungen wählen 182

Technologie zur Desinfektion einer aktiven Infektion 182

Verteilung der Computerressourcen bei der Virensuche 183

Aufgabenstart im Hintergrundmodus 183

Programmparameter bei der Arbeit im Vollbildmodus. Profil für Spiele 184

Energiesparen im Akkubetrieb 184

KATEGORIEN DER ERKENNBAREN BEDROHUNGEN WÄHLEN

Die Bedrohungen, die von Kaspersky Internet Security erkannt werden, sind nach unterschiedlichen Merkmalen in Kategorien angeordnet. Viren, trojanische Programme und schädliche Tools werden immer vom Programm erkannt. Diese Programme können Ihrem Computer ernsthaften Schaden zufügen. Zur Steigerung der Computersicherheit lässt sich die Liste der zu erkennenden Bedrohungen durch Aktivierung der Kontrolle des Verhaltens legaler Programme erweitern, die von Angreifern zur Schädigung des Computers oder der Daten des Benutzers verwendet werden können.

Gehen Sie folgendermaßen vor, um die Kategorien erkennbare Bedrohungen auszuwählen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Bedrohungen und Ausnahmen**.
3. Klicken Sie auf der rechten Fensterseite auf die unterhalb der Liste **Erkennung folgender Bedrohungstypen aktiviert** angeordnete Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster **Bedrohungen** die Kontrollkästchen für die Bedrohungen, die erkannt werden sollen.

TECHNOLOGIE ZUR DESINFEKTION EINER AKTIVEN INFEKTION

Moderne Schadprogramme können in die tiefste Ebene des Betriebssystems eindringen, wodurch es praktisch unmöglich wird, sie zu löschen. Wenn Kaspersky Internet Security eine schädliche Aktivität im System erkennt, bietet er an, einen speziell dafür vorgesehenen erweiterten Desinfektionsvorgang auszuführen, durch den die Bedrohung neutralisiert und vom Computer gelöscht wird.

Zum Abschluss des Vorgangs erfolgt ein obligatorischer Neustart des Computers. Nach dem Neustart des Computers wird empfohlen, eine vollständige Virenuntersuchung zu starten (s. Abschnitt "Wie eine vollständige Virenuntersuchung des Computers ausgeführt wird" auf S. 65).

Gehen Sie folgendermaßen vor, damit Kaspersky Internet Security die Prozedur zur erweiterten Desinfektion anwendet:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Kompatibilität**.
3. Aktivieren Sie das Kontrollkästchen **Technologie zur aktiven Desinfektion verwenden**.

VERTEILUNG DER COMPUTERRESSOURCEN BEI DER VIRENSUCHE

Um die Belastung des Prozessors und der Laufwerkssubsysteme zu reduzieren, können Sie festlegen, dass Aufgaben zur Virensuche aufgeschoben werden.

Das Ausführen von Untersuchungsaufgaben erhöht die Auslastung des Prozessors und der Laufwerkssubsysteme und verlangsamt dadurch die Arbeit anderer Programme. In der Grundeinstellung hält Kaspersky Internet Security beim Eintreten dieser Situation die Ausführung von Untersuchungsaufgaben an und gibt Systemressourcen für Benutzeranwendungen frei.

Allerdings existiert eine Reihe von Programmen, die gestartet werden, wenn Prozessorressourcen frei werden, und im Hintergrundmodus arbeiten. Wenn die Untersuchung von der Arbeit solcher Programme unabhängig sein soll, sollten ihnen keine Systemressourcen überlassen werden.

Beachten Sie, dass dieser Parameter für jede Untersuchungsaufgabe individuell angepasst werden kann. In diesem Fall besitzt der für eine konkrete Aufgabe festgelegte Parameter die höchste Priorität.

Gehen Sie folgendermaßen vor, damit Kaspersky Internet Security die Untersuchungsaufgaben zurückstellt, wenn sie die Arbeit anderer Programme verlangsamen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Kompatibilität**.
3. Aktivieren Sie das Kontrollkästchen **Ressourcen für andere Programme freigeben**.

AUFGABENSTART IM HINTERGRUNDMODUS

Um eine optimale Auslastung der Computerressourcen zu erreichen, können Sie eine regelmäßige Rootkit-Suche im Hintergrundmodus sowie den Start von ressourcenintensiven Aufgaben bei Computerleerlauf aktivieren.

Die regelmäßige Rootkit-Suche wird ausgeführt, während Sie mit dem Computer arbeiten. Die Suche dauert maximal 5 Minuten und erfordert minimale Computerressourcen.

Zu den Aufgaben die bei Leerlauf des Computers gestartet werden können, zählen:

- automatisches Update der Antiviren-Datenbanken und Programm-Module
- Untersuchung des Arbeitsspeichers, der Autostart-Objekte und der Systempartition

Die bei bei Computerleerlauf auszuführenden Aufgaben werden gestartet, wenn der Computer vom Benutzer gesperrt wurde oder der Bildschirmschoner länger als 5 Minuten angezeigt wird.

Wenn der Computer im Batteriebetrieb arbeitet, werden im Computerleerlauf keine Aufgaben gestartet.

Der erste Schritt für den Start von Aufgaben, die bei Computerleerlauf ausgeführt werden, besteht in einer Aktualitätsprüfung der Datenbanken und Programm-Module. Wenn sich daraus ergibt, dass eine Aktualisierung erforderlich ist, wird die Aufgabe zum automatischen Update gestartet. Beim zweiten Schritt werden Datum und Status der letzten Aufgabenausführung bei Computerleerlauf geprüft. Wenn die Aufgabe bei Computerleerlauf noch nicht gestartet wurde, länger als 7 Tage nicht ausgeführt wurde oder abgebrochen wurde, wird die Aufgabe zur Untersuchung des Arbeitsspeichers, der Autostart-Objekte und der Systemregistrierung gestartet.

Die Untersuchung bei Computerleerlauf wird mit einer tiefgehenden heuristischen Analyse ausgeführt, wodurch sich eine hohe Wahrscheinlichkeit für den Fund von versteckten Bedrohungen ergibt.

Die Aufgabe bei Computerleerlauf wird abgebrochen, wenn der Benutzer seine Arbeit fortsetzt. Dabei wird festgehalten, an welcher Stelle die Aufgabe abgebrochen wurde, um sie beim nächsten Mal dort fortzusetzen.

Wenn die Aufgabenausführung bei Computerleerlauf abgebrochen wurde, während ein Update heruntergeladen wurde, so wird die Aktualisierung beim nächsten Mal neu gestartet.

Gehen Sie folgendermaßen vor, eine regelmäßige Rootkit-Suche im Hintergrundmodus zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Untersuchung des Computers** den Abschnitt **Allgemeine Einstellungen**.
3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Regelmäßige Rootkit-Suche ausführen**.

Gehen Sie folgendermaßen vor, um die Ausführung von Aufgaben bei Computerleerlauf zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Untersuchung des Computers** den Abschnitt **Allgemeine Einstellungen**.
3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Untersuchung bei Computerleerlauf ausführen**.

PROGRAMMPARAMETER BEI DER ARBEIT IM VOLLBILDMODUS. PROFIL FÜR SPIELE

Die Verwendung bestimmter Programme (insbesondere von Computerspielen) im Vollbildmodus ist für die Kompatibilität mit einigen Funktionen von Kaspersky Internet Security problematisch. In diesem Modus sind beispielsweise Meldungsfenster unangebracht. Teilweise nehmen solche Programme auch erhebliche Systemressourcen in Anspruch, sodass die Ausführung einer Aufgabe von Kaspersky Internet Security zur einer Verlangsamung dieser Programme führen kann.

Damit der Benutzer nicht jedes Mal, wenn er in den Vollbildmodus wechselt, manuell die Benachrichtigungen deaktivieren und Aufgaben anhalten muss, bietet Kaspersky Internet Security die Möglichkeit, diese Parameter mit Hilfe eines Profils für Spiele vorübergehend zu ändern. Wenn das Spiele-Profils aktiviert wird, werden beim Wechsel in den Vollbildmodus automatisch die Parameter aller Komponenten so geändert, dass eine optimale Arbeit in diesem Modus gewährleistet ist. Bei Verlassen des Vollbildmodus werden für die Parameter des Programms die Werte wiederhergestellt, die vor dem Wechsel in den Vollbildmodus eingestellt waren.

Gehen Sie folgendermaßen vor, um die Verwendung des Profils für Spiele zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Profil für Spiele**.
3. Aktivieren Sie das Kontrollkästchen **Profil für Spiele verwenden** und geben Sie darunter im Block **Einstellungen für Profil** die erforderlichen Einstellungen für die Verwendung des Spiele-Profils an.

ENERGIESPAREN IM AKKUBETRIEB

Um sparsam mit der Batterie eines Laptops umzugehen, können Sie Aufgaben zur Virensuche und zum Update nach Zeitplan aufschieben. Bei Bedarf können Sie Kaspersky Internet Security auf Befehl aktualisieren oder die Virenuntersuchung manuell starten.

Gehen Sie folgendermaßen vor, um den Energiesparmodus bei Akkubetrieb zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Energiesparen**.

3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Geplante Untersuchungsaufgaben bei Akkubetrieb nicht starten**.

SELBSTSCHUTZ FÜR KASPERSKY INTERNET SECURITY

Da Kaspersky Internet Security für die Sicherheit des Computers vor schädlichen Programmen verantwortlich ist, versuchen bestimmte Schadprogramme, die auf den Computer gelangen, die Arbeit von Kaspersky Internet Security zu blockieren oder ihn sogar vom Computer zu löschen.

Die Stabilität des Sicherheitssystems für Ihren Computer wird in Kaspersky Internet Security durch Mechanismen zum Selbstschutz und zum Schutz vor externem Zugriff realisiert.

Der Selbstschutz für Kaspersky Internet Security verhindert, dass seine Dateien auf der Festplatte, Prozesse im Speicher und Einträge in der Registrierung verändert oder gelöscht werden. Der Schutz vor externem Zugriff kann alle Versuche zur Fernsteuerung der Programmdienste blockieren.

Für 64-Bit-Betriebssysteme und für Microsoft Windows Vista steht der Selbstschutzmechanismus von Kaspersky Internet Security nur im Hinblick auf Veränderungen oder Löschen von eigenen Dateien auf der Festplatte und Veränderungen oder Löschen von Einträgen in der Systemregistrierung zur Verfügung.

IN DIESEM ABSCHNITT

Selbstschutz aktivieren und deaktivieren 185

Schutz vor externer Steuerung..... 185

SELBSTSCHUTZ AKTIVIEREN UND DEAKTIVIEREN

Der Selbstschutz von Kaspersky Internet Security ist standardmäßig aktiviert. Bei Bedarf können Sie den Selbstschutz deaktivieren.

Gehen Sie folgendermaßen vor, um den Selbstschutz von Kaspersky Internet Security zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Selbstschutz**.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **Selbstschutz aktivieren**.

SCHUTZ VOR EXTERNER STEUERUNG

Der Schutz vor externer Steuerung ist standardmäßig aktiviert. Bei Bedarf können Sie den Schutz deaktivieren.

Wenn der Schutz vor Fernsteuerung aktiviert ist, kann es vorkommen, dass gleichzeitig Programme, die der Remote-Administration dienen, eingesetzt werden sollen (z.B. RemoteAdmin). Um die Arbeit dieser Programme zu ermöglichen, werden sie zur Liste der vertrauenswürdigen Programme (s. Abschnitt "Liste mit vertrauenswürdigen Programmen erstellen" auf S. 180) hinzugefügt, und die Einstellung **Programmaktivität nicht kontrollieren** wird für sie aktiviert.

Gehen Sie folgendermaßen vor, um den Schutz vor externer Steuerung zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Selbstschutz**.

3. Deaktivieren Sie im Block **Externe Steuerung** das Kontrollkästchen **Option zur externen Steuerung des Systemdienstes deaktivieren**.

QUARANTÄNE UND BACKUP

Die *Quarantäne* ist ein spezieller Speicher, in den Objekte verschoben werden, die möglicherweise von Viren infiziert sind. *Möglicherweise infizierte Objekte* sind Objekte, die verdächtig sind, von Viren oder Virenmodifikationen infiziert zu sein.

Ein verdächtiges Objekt kann während der Virensuche sowie bei der Arbeit von Datei-Anti-Virus, Mail-Anti-Virus und Proaktiver Schutz gefunden und in die Quarantäne verschoben werden.

Objekte werden in folgenden Fällen in die Quarantäne verschoben:

- Der Objektcode besitzt Ähnlichkeit mit einer bekannten Bedrohung, wurde aber teilweise verändert, oder er erinnert an die Struktur eines Schadprogramms, ist aber nicht in den Datenbanken enthalten. In diesem Fall werden Objekte aufgrund einer heuristischen Analyse, die von Datei-Anti-Virus oder Mail-Anti-Virus ausgeführt wird oder bei einer Virensuche erfolgt, in die Quarantäne verschoben. Der heuristische Analysemechanismus führt nur selten zu einem Fehlalarm.

- Die Aktionsfolge, die von einem Objekt ausgeführt werden soll, gilt als verdächtig. In diesem Fall werden Objekte aufgrund einer Verhaltensanalyse, die vom Proaktiven Schutz ausgeführt wird, in die Quarantäne verschoben.

Ein Objekt unter Quarantäne zu stellen, bedeutet, es wird nicht kopiert, sondern verschoben: Das Objekt wird am ursprünglichen Speicherort oder aus einer E-Mail-Nachricht gelöscht und im Quarantäneordner gespeichert. Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

Das *Backup* dient zur Speicherung der Sicherungskopien für infizierte Objekte, die zum Zeitpunkt ihrer Entdeckung nicht desinfiziert werden können.

Möglicherweise kann die Bedrohung von Kaspersky Internet Security eindeutig bestimmt und desinfiziert werden, nachdem die Programm-Datenbanken aktualisiert wurden. Deshalb untersucht das Programm die Quarantäneobjekte nach jedem Update (s. S. 96).

IN DIESEM ABSCHNITT

Quarantäne- und Backup-Objekte speichern 186

Arbeit mit Objekten in der Quarantäne 187

QUARANTÄNE- UND BACKUP-OBJEKTE SPEICHERN

Die maximale Speicherdauer für Objekte beträgt standardmäßig 30 Tage. Danach werden die Objekte gelöscht. Sie können diese Zeitbeschränkung aufheben oder die maximale Speicherdauer für Objekte ändern.

Außerdem können Sie eine maximale Größe für die Quarantäne und das Backup festlegen. Beim Erreichen der maximalen Größe wird der Inhalt der Quarantäne und des Backups durch neue Objekte ersetzt. Die Größenbeschränkung ist standardmäßig deaktiviert.

➡ *Gehen Sie folgendermaßen vor, um eine maximale Speicherdauer für Objekte festzulegen:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Berichte und Speicher**.

3. Aktivieren Sie auf der rechten Fensterseite im Block **Quarantäne- und Backup-Objekte speichern** das Kontrollkästchen **Objekte speichern für maximal** und legen Sie eine maximale Speicherdauer für Quarantäneobjekte fest.

Gehen Sie folgendermaßen vor, um diee maximale Größe für die Quarantäne und das Backup anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Berichte und Speicher**.

3. Aktivieren Sie auf der rechten Fensterseite im Block **Quarantäne- und Backup-Objekte speichern** das Kontrollkästchen **Maximale Größe** und legen Sie eine maximale Größe für die Quarantäne und das Backup fest.

ARBEIT MIT OBJEKTEN IN DER QUARANTÄNE

Die Quarantäne von Kaspersky Internet Security ermöglicht die Ausführung folgender Operationen:

- Dateien, die Sie für infiziert halten, in die Quarantäne verschieben.
- Untersuchung und Desinfektion aller potentiell infizierten Objekte der Quarantäne unter Nutzung der aktuellen Datenbankversion von Kaspersky Internet Security.
- Wiederherstellung von Dateien in einem vom Benutzer gewählten Ordner oder (standardmäßig) in den Ordnern, aus denen sie in die Quarantäne verschoben wurden.
- Ein beliebiges Quarantäneobjekt oder eine Gruppe der Objekte löschen.
- Quarantäneobjekte zur Untersuchung an Kaspersky Lab schicken.

Ein Objekt kann auf zwei Arten in die Quarantäne verschoben werden:

- mit dem Link **In die Quarantäne verschieben** im Fenster **Schutzstatus**.
- mit Hilfe des Kontextmenüs für ein Objekt

Gehen Sie folgendermaßen vor, um vom Fenster Schutzstatus aus ein Objekt in die Quarantäne zu verschieben:

1. Öffnen Sie das Programmhauptfenster.

2. Klicken Sie im Hauptfenster oben auf den Link **Quarantäne**, um das Fenster **Schutzstatus** auf der Registerkarte **Erkannte Bedrohungen** zu öffnen.

3. Klicken Sie auf **In Quarantäne verschieben**.

4. Wählen Sie im folgenden Fenster das Objekt, das in die Quarantäne verschoben werden soll.

Gehen Sie folgendermaßen vor, um ein Objekt mit Hilfe des Kontextmenüs in die Quarantäne zu verschieben:

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und gehen Sie in den Ordner mit dem Objekt, das in die Quarantäne verschoben werden soll.

2. Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt und wählen Sie den Punkt **In die Quarantäne verschieben**.

Gehen Sie folgendermaßen vor, um ein Objekt in der Quarantäne zu untersuchen:

1. Öffnen Sie das Programmhauptfenster .

2. Betätigen Sie den Link **Quarantäne** im oberen Fensterbereich und öffnen Sie das Quarantänefenster.

3. Wählen Sie im folgenden Fenster auf der Registerkarte **Erkannte Bedrohungen** das zu untersuchende Objekt aus.

4. Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt und wählen Sie dort den Punkt **Untersuchen**.

Gehen Sie folgendermaßen vor, um eine Desinfektion aller Objekte in der Quarantäne durchzuführen:

1. Öffnen Sie das Programmhauptfenster.

2. Betätigen Sie den Link **Quarantäne** im oberen Fensterbereich und öffnen Sie das Quarantänefenster.

3. Klicken Sie im folgenden Fenster auf der Registerkarte **Erkannte Bedrohungen** auf die Schaltfläche **Alle desinfizieren**.

Gehen Sie folgendermaßen vor, um eine Datei aus der Quarantäne wiederherzustellen:

1. Öffnen Sie das Programmhauptfenster.

2. Betätigen Sie den Link **Quarantäne** im oberen Fensterbereich und öffnen Sie das Quarantänefenster.

3. Wählen Sie im folgenden Fenster auf der Registerkarte **Erkannte Bedrohungen** das wiederherzustellende Objekt aus.

4. Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt und wählen Sie dort den Punkt **Wiederherstellen** aus.

Gehen Sie folgendermaßen vor, um Objekte aus der Quarantäne zu entfernen:

1. Öffnen Sie das Programmhauptfenster.

2. Betätigen Sie den Link **Quarantäne** im oberen Fensterbereich und öffnen Sie das Quarantänefenster.

3. Wählen Sie im folgenden Fenster auf der Registerkarte **Erkannte Bedrohungen** das zu entfernende Objekt aus.

4. Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt und wählen Sie dort den Punkt **Aus der Liste löschen** aus.

Um ein Quarantäneobjekt zur Untersuchung an Kaspersky Lab zu schicken, gehen Sie wie folgt vor.

1. Öffnen Sie das Programmhauptfenster.

2. Betätigen Sie den Link **Quarantäne** im oberen Fensterbereich und öffnen Sie das Quarantänefenster.

3. Wählen Sie im folgenden Fenster auf der Registerkarte **Erkannte Bedrohungen** das Objekt aus, das zur Untersuchung geschickt werden soll.

4. Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt und wählen Sie dort den Punkt **Senden**.

ZUSÄTZLICHE SCHUTZ-TOOLS

Zum Lieferumfang von Kaspersky Internet Security gehören verschiedene Assistenten und Tools, mit denen Aufgaben für die Computersicherheit gelöst werden.

- Der Assistent zum Erstellen einer Notfall-CD dient dazu, eine Notfall-CD zu erstellen, mit der sich die Funktionsfähigkeit des Systems nach einem Virenangriff durch Booten von einem Wechseldatenträger wiederherstellen lässt. Die Notfall-CD kommt dann zum Einsatz, wenn der Infektionsgrad so hoch ist, dass die Desinfektion eines Computers nicht mehr mit Hilfe von Antiviren-Anwendungen oder Desinfektionstools möglich ist.

- Der Assistent zum Löschen von Aktivitätsspuren dient dazu, im System nach Aktivitätsspuren eines Benutzers sowie auch nach Betriebssystemparametern, die zum Sammeln von Informationen über die Aktivität des Benutzers dienen, zu suchen und diese zu beseitigen.

- Der Assistent zur Systemwiederherstellung dient dazu, Beschädigungen des Systems und die Spuren von schädlichen Objekten im System zu beseitigen.

- Der Assistent zur Browser-Konfiguration dient dazu, die Parameter des Browsers Microsoft Internet Explorer zu analysieren und anzupassen, um potentielle Schwachstellen zu beseitigen.

- Die Schwachstellensuche dient zur Diagnose des Betriebssystems und der installierten Programme, um Schwachstellen festzustellen, die von Angreifern ausgenutzt werden können.

Alle Probleme, die von den Assistenten gefunden werden (unter Ausnahme des Assistenten zum Erstellen einer Notfall-CD) werden im Hinblick auf die von ihnen für das System ausgehende Gefahr eingeteilt. Für jede Gruppe von Problemen schlagen die Kaspersky-Lab-Spezialisten eine Auswahl von Aktionen vor, mit denen die Schwachstellen und kritischen Punkte im System behoben werden können. Die Probleme und die entsprechenden Aktionen werden in drei Gruppen unterteilt:

- *Ausdrücklich empfohlene Aktionen* können Probleme beheben, die eine ernsthafte Sicherheitsbedrohung darstellen. Es wird empfohlen, alle Aktionen dieser Gruppe rechtzeitig auszuführen, um die Bedrohungen zu beseitigen.

- *Empfohlene Aktionen* dienen zum Beheben von Problemen, die ein potentielles Risiko darstellen können. Um einen optimalen Schutz zu gewährleisten, sollten auch die Aktionen dieser Gruppe ausgeführt werden.

- *Zusätzliche Aktionen* dienen dazu, momentan ungefährliche Probleme zu beheben, die die Computersicherheit aber in Zukunft bedrohen können. Diese Vorgehensweise sorgt für einen vollständigen Schutz Ihres Computers, kann aber in einigen Fällen zu einem Löschen von Benutzerparametern (z.B. von Cookies) führen.

IN DIESEM ABSCHNITT

Aktivitätsspuren löschen 189

Browser-Konfiguration 191

Rollback von Änderungen, die von den Assistenten ausgeführt wurden 192

AKTIVITÄTSSPUREN LÖSCHEN

Während der Arbeit auf dem Computer werden die Aktionen des Benutzers im System registriert. Dabei werden Daten darüber gespeichert, welche Suchanfragen der Benutzer vornimmt, welche Seiten er besucht, welche Programme er startet und welche Dateien er öffnet und speichert. Außerdem werden Einträge im Systemjournal von Microsoft Windows, temporäre Dateien u.v.a gespeichert.

Alle genannten Informationsquellen über die Benutzeraktivität können sensible Daten (darunter auch Kennwörter) enthalten und können unter Umständen von Angreifern entwendet und analysiert werden. Viele Benutzer verfügen nicht über ausreichende Kenntnisse, um einem Diebstahl wertvoller Informationen aus solchen Quellen vorzubeugen.

Kaspersky Internet Security verfügt über einen Assistenten zum Löschen von Aktivitätsspuren. Dieser Assistent führt im System die Suche nach Spuren von Benutzeraktivität und den Betriebssystemsparametern, die zum Sammeln von Informationen über die Aktivität dienen, durch.

Es sollte beachtet werden, dass laufend Informationen über die Aktivität des Benutzers im System gesammelt werden. Der Start einer beliebigen Datei oder das Öffnen eines Dokuments werden in einem Verlauf festgehalten, und das Systemjournal von Microsoft Windows registriert eine Vielzahl von Ereignissen, die im System vorfallen. Deshalb kann es sein, dass bei einem wiederholten Start des Assistenten zum Löschen von Aktivitätsspuren gefunden werden, die beim vorhergehenden Start des Assistenten bereits gelöscht worden sind. Es kann vorkommen, dass bestimmte Dateien, wie z.B. eine Journaldatei von Microsoft Windows, vom System verwendet werden, während sie vom Assistenten gelöscht werden sollen. Um diese Dateien zu löschen, schlägt der Assistent vor, das System neu zu starten. Im Verlauf eines Neustarts können solche Dateien aber erneut erstellt werden, was dazu führt, dass sie wieder als Aktivitätsspuren erkannt werden.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Gehen Sie folgendermaßen vor, den Assistenten zum Löschen von Aktivitätsspuren zu starten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Tools**.
2. Klicken Sie auf der rechten Fensterseite auf Löschen von Aktivitätsspuren.

Details zu den einzelnen Schritte des Assistenten

Schritt 1. Assistent starten

Vergewissern Sie sich, dass die Variante **Diagnose der Spuren von Benutzeraktivität durchführen** gewählt wurde, und klicken Sie auf **Weiter**, um den Assistenten zu starten.

Schritt 2. Suche von Aktivitätsspuren

Der Assistent führt auf Ihrem Computer die Suche nach Aktivitätsspuren aus. Die Suche kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 3. Aktionen für das Löschen von Aktivitätsspuren wählen

Nach dem Abschluss der Suche informiert der Assistent über die gefundenen Aktivitätsspuren und mögliche Aktionen, um sie zu beseitigen. Der Bericht über die Arbeit des Assistenten besteht aus einer Tabelle (s. Abschnitt "Zusätzliche Schutz-Tools" auf S. 188).

Klicken Sie links vom Namen einer Gruppe auf das Zeichen **+**, um die Aktionen der Gruppe anzuzeigen.

Um eine bestimmte Aktion auszuführen, aktivieren Sie das Kontrollkästchen links vom Namen der Aktion. In der Grundeinstellung werden alle empfohlenen und ausdrücklich empfohlenen Aktionen ausgeführt. Soll eine bestimmte Aktion nicht ausgeführt werden, dann deaktivieren Sie das entsprechende Kontrollkästchen

Die standardmäßig aktivierten Kontrollkästchen sollten auf keinen Fall entfernt werden, weil dadurch die Sicherheit Ihres Computers bedroht wird.

Klicken Sie auf **Weiter**, nachdem Sie die Aktionen gewählt haben, die der Assistent ausführen soll.

Schritt 4. Aktivitätsspuren löschen

Der Assistent führt die Aktionen aus, die beim vorherigen Schritt festgelegt wurden. Das Löschen von Aktivitätsspuren kann eine gewisse Zeit beanspruchen. Um bestimmte Aktivitätsspuren zu löschen, kann ein Neustart des Computers erforderlich sein. Darüber werden Sie vom Assistenten informiert.

Der Assistent geht nach Abschluss des Löschens von Aktivitätsspuren automatisch zum nächsten Schritt.

Schritt 5. Assistent abschließen

Damit das Löschen von Aktivitätsspuren in Zukunft automatisch erfolgt, wenn Kaspersky Internet Security beendet wird, aktivieren Sie beim letzten Schritt des Assistenten das Kontrollkästchen **Löschen von Aktivitätsspuren jedes Mal beim Beenden von Kaspersky Internet Security ausführen**. Wenn Sie planen, die Aktivitätsspuren künftig selbst zu beseitigen, lassen Sie dieses Kontrollkästchen deaktiviert.

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

BROWSER-KONFIGURATION

In bestimmten Fällen ist es notwendig, den Browser Microsoft Internet Explorer auf spezielle Weise zu analysieren und anzupassen, da benutzerdefinierte oder standardmäßige Parameter zu Sicherheitsproblemen führen können.

Beispiele für Objekte und Parameter, die vom Browser verwendet werden und potentielle Sicherheitsrisiken bergen:

- **Zwischenspeicher für die Arbeit von Microsoft Internet Explorer**. Im Cache werden Daten gespeichert, die aus dem Internet heruntergeladen wurden. So lässt sich ein erneuter Download vermeiden. Dadurch wird die Ladedauer für Webseiten reduziert und der Internet-Datenverkehr verringert. Allerdings enthält der Zwischenspeicher vertrauliche Daten und kann außerdem Aufschluss darüber geben, welche Ressourcen ein Benutzer besucht hat. Viele schädliche Objekte lesen beim Scannen der Festplatte auch den Zwischenspeicher. Auf diese Weise können Angreifer beispielsweise die Mailadressen von Benutzern erhalten. Zur Optimierung des Schutzes wird empfohlen, den Zwischenspeicher zu leeren, wenn die Arbeit mit dem Browser beendet wird.

- **Anzeige von Erweiterungen für dem System bekannte Dateitypen**. Um das Umbenennen von Dateien zu erleichtern, können die Erweiterungen ausgeblendet werden. Allerdings ist es für den Benutzer manchmal besser, die tatsächliche Dateierweiterung zu sehen. Häufig werden in den Namen schädlicher Objekte Zeichenfolgen verwendet, in denen der echten Erweiterung zu Imitationszwecken eine zusätzliche Erweiterung vorangestellt wird (z.B. example.txt.com). Wenn die tatsächliche Dateierweiterung nicht angezeigt wird, sieht der Benutzer nur den Teil des Dateinamens, der die imitierte Erweiterung enthält, und kann das schädliche Objekt für eine unschädliche Datei halten. Zur Optimierung des Schutzes wird empfohlen, die Anzeige von Erweiterungen für Dateien bekannter Formate zu aktivieren.

- **Liste mit vertrauenswürdigen Seiten**. Um problemlos mit bestimmten Webseiten arbeiten zu können, müssen sie der vertrauenswürdigen Liste hinzugefügt werden. Allerdings können schädliche Objekte können einer solchen Liste Links zu Webseiten hinzufügen, die von Angreifern erstellt wurden.

Es sollte berücksichtigt werden, dass bestimmte Parameterwerte zu Problemen bei der Anzeige spezieller Webseiten führen können (beispielsweise wenn sie ActiveX-Elemente verwenden). Das Problem lässt sich lösen, indem solche Webseiten in die vertrauenswürdige Zone aufgenommen werden.

Die Analyse und Konfiguration wird vom Assistenten zur Browser-Konfiguration ausgeführt. Der Assistent prüft, ob die aktuellen Updates für den Browser installiert sind und ob die Browser-Einstellungen keine Schwachstellen aufweisen, die das System verletzbar machen. Beim Abschluss des Assistenten wird ein Bericht erstellt, der zur Analyse an Kaspersky Lab geschickt werden kann.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Schließen Sie alle Browserfenster von Microsoft Internet Explorer, bevor mit der Diagnose begonnen wird.

➡ *Gehen Sie folgendermaßen vor, den Assistenten zur Browser-Konfiguration zu starten:*

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Tools**.
2. Klicken Sie auf der rechten Fensterseite auf
3. **Browser-Konfiguration**.

Details zu den einzelnen Schritte des Assistenten

Schritt 1. Assistent starten

Vergewissern Sie sich, dass die Variante **Diagnose von Microsoft Internet Explorer durchführen** gewählt wurde, und klicken Sie auf **Weiter**, um den Assistenten zu starten.

Schritt 2. Analyse der Einstellungen von Microsoft Internet Explorer

Der Assistent analysiert die Einstellungen des Browsers Microsoft Internet Explorer. Die Suche nach Problemen in den Einstellungen des Browsers kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 3. Aktionen für die Browser-Konfiguration wählen

Alle Probleme, die beim vorherigen Schritt gefunden wurden, werden im Hinblick auf ihre Gefährlichkeit für das System (s. Abschnitt "Zusätzliche Schutz-Tools" auf S. 188) eingeteilt.

Klicken Sie links vom Namen einer Gruppe auf das Zeichen **+**, um die Aktionen der Gruppe anzuzeigen.

Um eine bestimmte Aktion auszuführen, aktivieren Sie das Kontrollkästchen links vom Namen der Aktion. In der Grundeinstellung werden alle empfohlenen und ausdrücklich empfohlenen Aktionen ausgeführt. Soll eine bestimmte Aktion nicht ausgeführt werden, dann deaktivieren Sie das entsprechende Kontrollkästchen

Die standardmäßig aktivierten Kontrollkästchen sollten auf keinen Fall entfernt werden, weil dadurch die Sicherheit Ihres Computers bedroht wird.

Klicken Sie auf **Weiter**, nachdem Sie die Aktionen gewählt haben, die der Assistent ausführen soll.

Schritt 4. Browser-Konfiguration

Der Assistent führt die Aktionen aus, die beim vorherigen Schritt festgelegt wurden. Die Browser-Konfiguration kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Konfiguration automatisch zum nächsten Schritt.

Schritt 5. Assistent abschließen

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

ROLLBACK VON ÄNDERUNGEN, DIE VON DEN ASSISTENTEN AUSGEFÜHRT WURDEN

Bestimmte Änderungen, die beim Start des Assistenten zum Löschen von Aktivitätsspuren (s. Abschnitt "Aktivitätsspuren löschen" auf S. 189), des Assistenten zur Systemwiederherstellung (s. Abschnitt "Was tun, wenn Sie vermuten, dass Ihr Computer infiziert ist?" auf S. 71) und des Assistenten zur Browser-Konfiguration (s. Abschnitt "Browser-Konfiguration" auf S. 191) ausgeführt wurden, können rückgängig gemacht werden.

Starten Sie den entsprechenden Assistenten, um die Veränderungen rückgängig zu machen:

1. Öffnen Sie das Programmhauptfenster und wählen Sie auf der linken Fensterseite den Abschnitt **Tools**.
2. Klicken Sie auf der rechten Fensterseite auf eine der folgenden Schaltflächen:
   - **Löschen von Aktivitätsspuren** – für den Start des Assistenten zum Löschen von Aktivitätsspuren.
   - **Wiederherstellung nach Infektion** – für den Start des Assistenten zur Systemwiederherstellung.

- **Browser-Konfiguration** – für den Start des Assistenten zur Browser-Konfiguration.

Im Folgenden wird beschrieben, welche Schritte der Assistent bei einem Rollback von Veränderungen ausführt.

Schritt 1. Assistent starten

Wählen Sie die Variante **Änderungen verwerfen** und klicken Sie auf **Weiter**.

Schritt 2. Änderungen suchen

Der Assistent sucht nach Veränderungen, die er früher ausgeführt hat und für die ein Rollback möglich ist. Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 3. Veränderungen wählen, die zurückgenommen werden sollen.

Bei diesem Schritt wird über die gefundenen Veränderungen informiert. Der Bericht besteht aus einer Liste und enthält auch die früher vom Assistenten ausgeführten Aktionen, die rückgängig gemacht werden können.

Aktivieren Sie das Kontrollkästchen für die entsprechende Aktion, damit der Assistent eine früher ausgeführte Aktion zurücknimmt.

Klicken Sie auf **Weiter**, nachdem Sie die Aktionen für das Rollback gewählt haben.

Schritt 4. Rollback der Änderungen

Der Assistent macht die beim vorherigen Schritt gewählten Aktionen rückgängig. Der Assistent geht nach dem Rollback der Änderungen automatisch zum nächsten Schritt.

Schritt 5. Assistent abschließen

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

BERICHTE

Die Ereignisse, die während der Arbeit der Schutzkomponenten oder bei der Ausführung von Aufgaben von Kaspersky Internet Security eintreten, werden in Berichten festgehalten. Sie können für jede Schutzkomponente oder Aufgabe einen detaillierten Bericht erstellen und die Darstellung der Daten anpassen. Außerdem können Sie die Daten filtern (s. Abschnitt "Datenfilterung" auf S. 194) und in einem Bericht nach Ereignissen suchen (s. Abschnitt "Suche nach Ereignissen" auf S. 195).

Falls erforderlich, können Sie die Daten eines Berichts in einer Textdatei speichern (s. Abschnitt "Bericht in Datei speichern" auf S. 196). Außerdem können Sie die Berichte, deren Daten Sie nicht mehr benötigen, leeren (s. Abschnitt "Berichte leeren" auf S. 196) und die Parameter für das Erstellen (s. Abschnitt "Nicht kritische Ereignisse protokollieren" auf S. 197) und Speichern von Berichten (s. Abschnitt "Berichte speichern" auf S. 196) anpassen.

IN DIESEM ABSCHNITT

Bericht für eine bestimmte Komponente erstellen 194

Datenfilterung 194

Suche nach Ereignissen 195

Bericht in Datei speichern 196

Berichte speichern 196

Berichte leeren 196

Nicht kritische Ereignisse protokollieren 197

Erinnerung an die Bereitschaft eines Berichts anpassen 197

BERICHT FÜR EINE BESTIMMTE KOMPONENTE ERSTELLEN

Sie können einen detallierten Bericht über die Ereignisse erhalten, die bei der Arbeit der einzelnen Komponenten und Aufgaben von Kaspersky Internet Security eintreten.

Zur übersichtlichen Arbeit mit Berichten können Sie die Darstellung von Daten auf dem Bildschirm ändern: Ereignisse nach unterschiedlichen Parametern anordnen, Berichtszeitraum wählen, Ereignisse nach einer Spalte oder nach Priorität anordnen, Tabellenspalten ausblenden.

Gehen Sie folgendermaßen vor, um einen Bericht für eine Komponente oder Aufgabe zu erhalten:

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie mit dem Link **Berichte** im oberen Fensterbereich das Fenster für Berichte.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Detaillierter Bericht**.
4. Wählen Sie im folgenden Fenster **Detaillierter Bericht** links eine Komponente oder Aufgabe, für die ein Bericht erstellt werden soll. Bei Auswahl des Punkts **Schutz-Center** wird ein Bericht für alle Schutzkomponenten erstellt.

DATENFILTERUNG

Die Ereignisse in den Berichten für Kaspersky Internet Security können nach einem oder mehreren Werten in den Tabellenspalten gefiltert werden. Außerdem lassen sich komplexe Bedingungen für die Datenfilterung festlegen.

Gehen Sie folgendermaßen vor, um die Ereignisse nach Werten zu filtern:

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie mit dem Link **Berichte** im oberen Fensterbereich das Fenster für Berichte.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Detaillierter Bericht**.
4. Zeigen Sie auf der rechten Seite des folgenden Fensters **Detaillierter Bericht** mit der Maus auf die linke obere Ecke der Überschrift einer Tabellenspalte und öffnen Sie durch Linksklick das Filtermenü.
5. Wählen Sie im Filtermenü den Wert, nach dem die Daten gefiltert werden sollen.

6. Wiederholen Sie den Vorgang bei Bedarf für eine andere Tabellenspalte.

Gehen Sie folgendermaßen vor, um eine komplexe Filterbedingung festzulegen:

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie mit dem Link **Berichte** im oberen Fensterbereich das Fenster für Berichte.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Detaillierter Bericht**.
4. Öffnen Sie auf der rechten Seite des folgenden Fensters **Detaillierter Bericht** durch Rechtsklick das Kontextmenü für die entsprechende Berichtspalte und wählen Sie dort den Punkt **Filter**.
5. Legen Sie im folgenden Fenster **Komplexer Filter** die Filterbedingungen fest.
   a. Legen Sie auf der rechten Fensterseite die Auswahlgrenzen fest.
   b. Wählen Sie auf der linken Fensterseite in der Dropdown-Liste **Bedingung** eine Auswahlbedingung fest (z.B.: größer oder kleiner, gleich oder ungleich mit dem Wert, der als Auswahlgrenze angegeben wurde).
   c. Fügen Sie bei Bedarf eine zweite Bedingung hinzu. Verwenden Sie dazu die logischen Operationen Konjunktion (logisches UND) und Disjunktion (logisches ODER). Wenn Sie möchten, dass er Datenzugriff beide festgelegte Bedingungen erfüllt, wählen Sie **UND** aus. Ist eine Bedienung ausreichend, dann wählen Sie **ODER** aus.

SUCHE NACH EREIGNISSEN

Um in einem Bericht nach einem bestimmten Ereignis zu suchen, können Sie entweder in der Suchzeile oder in einem speziellen Fenster ein Schlüsselwort eingeben.

Gehen Sie folgendermaßen vor, um mit der Suchzeile nach einem Ereignis zu suchen:

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie mit dem Link **Berichte** im oberen Fensterbereich das Fenster für Berichte.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Detaillierter Bericht**.
4. Geben Sie auf der rechten Seite des folgenden Fensters **Detaillierter Bericht** in der Suchzeile ein Schlüsselwort ein.

Gehen Sie folgendermaßen vor, um mit dem Suchfenster nach einem Ereignis zu suchen:

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie mit dem Link **Berichte** im oberen Fensterbereich das Fenster für Berichte.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Detaillierter Bericht**.
4. Öffnen Sie auf der rechten Seite des folgenden Fensters **Detaillierter Bericht** durch Rechtsklick das Kontextmenü für die Überschrift der entsprechenden Spalte und wählen Sie dort den Punkt **Suche**.
5. Legen Sie im folgenden **Fenster** Suche die Suchkriterien fest.
   a. Geben Sie im Feld **Zeile** das gesuchte Schlüsselwort ein.
   b. Wählen Sie in der Dropdown-Liste **Spalte** den Namen der Spalte, in der nach dem angegebenen Schlüsselwort gesucht werden soll.
   c. Aktivieren Sie bei Bedarf die Kontrollkästchen für zusätzliche Suchparameter.

6. Klicken Sie auf **Weitersuchen**.

BERICHT IN DATEI SPEICHERN

Der Bericht kann in einer Textdatei gespeichert werden.

Gehen Sie folgendermaßen vor, um den Bericht in einer Datei zu speichern:

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie mit dem Link **Berichte** im oberen Fensterbereich das Fenster für Berichte.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Detaillierter Bericht**.
4. Erstellen Sie im folgenden Fenster **Detaillierter Bericht** den gewünschten Bericht und klicken Sie auf **Speichern**.
5. Geben Sie im folgenden Fenster den Ordner an, in dem die Berichtsdatei gespeichert werden soll, und nennen Sie einen Dateinamen.

BERICHTE SPEICHERN

Die standardmäßige Speicherdauer für Ereignisberichte beträgt 30 Tage. Danach werden die Daten gelöscht. Sie können diese Zeitbeschränkung aufheben oder die maximale Speicherdauer für Berichte ändern.

Außerdem können Sie eine maximale Größe für eine Berichtsdatei festlegen. Die maximale Größe beträgt standardmäßig 1024 MB. Beim Erreichen der maximalen Größe wird der Inhalt der Datei durch neue Einträge ersetzt. Sie können die Größenbeschränkung aufheben oder einen anderen Wert festlegen.

Gehen Sie folgendermaßen vor, um eine maximale Speicherdauer für Ereignisberichte festzulegen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Berichte und Speicher**.
3. Aktivieren Sie auf der rechten Fensterseite im Block **Berichte speichern** das Kontrollkästchen **Berichte speichern für maximal** und legen Sie eine maximale Speicherdauer für Berichte fest.

Gehen Sie folgendermaßen vor, um die maximale Größe einer Berichtsdatei festzulegen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Berichte und Speicher**.
3. Aktivieren Sie auf der rechten Fensterseite im Block **Berichte speichern** das Kontrollkästchen **Maximale Dateigröße** und legen Sie die maximale Größe einer Berichtsdatei fest.

BERICHTE LEEREN

Berichte, deren Daten Sie nicht mehr benötigen, können bereinigt werden.

Um die Berichte zu leeren*, machen Sie Folgendes*:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Berichte und Speicher**.

3. Klicken Sie auf der rechten Fensterseite im Block **Berichte leeren** auf **Leeren**.

4. Aktivieren Sie im folgenden Fenster **Informationen aus Berichten löschen** die Kontrollkästchen der Berichte, die Sie bereinigen möchten.

NICHT KRITISCHE EREIGNISSE PROTOKOLLIEREN

Einträge über nicht kritische Ereignisse sowie Ereignisse, die die Registrierung und das Dateisystem betreffen, werden in der Grundeinstellung nicht protokolliert. Sie können solche Einträge in den Schutzbericht aufnehmen.

Gehen Sie folgendermaßen vor, um die Protokollierung von nicht kritischen Ereignissen zu aktivieren:

1. Öffdas Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Berichte und Speicher**.

3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Protokollierung von nicht kritischen Ereignisse aktivieren**.

ERINNERUNG AN DIE BEREITSCHAFT EINES BERICHTS ANPASSEN

Sie können einen Zeitplan erstellen, nach dem Kaspersky Internet Security Sie über die Bereitschaft eines Berichts benachrichtigen soll.

Gehen Sie folgendermaßen vor, um einen Zeitplan zu erstellen:

1. Öffnen Sie das Programmhauptfenster.

2. Öffnen Sie mit dem Link **Berichte** im oberen Fensterbereich das Fenster für Berichte.

3. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Bericht** das Kontrollkästchen **An Bericht erinnern** und klicken Sie auf den Link mit dem eingestellten Zeitpunkt, um das Zeitplanfenster zu öffnen.

4. Stellen Sie im folgenden Fenster **Bericht: Zeitplan** den Zeitplan ein.

AUSSEHEN DES PROGRAMMS

Sie können das Aussehen von Kaspersky Internet Security verändern, indem Sie alternative grafische Oberflächen verwenden. Zusätzlich besteht die Möglichkeit, aktive Elemente der Benutzeroberfläche anzupassen (Programmsymbol im Infobereich der Microsoft Windows-Taskleiste und Popupmeldungen).

IN DIESEM ABSCHNITT

Grafische Oberfläche von Kaspersky Internet Security 198

Aktive Elemente der Benutzeroberfläche 198

News Agent 198

GRAFISCHE OBERFLÄCHE VON KASPERSKY INTERNET SECURITY

Alle auf der Oberfläche von Kaspersky Internet Security verwendeten Farben, Schriften, Piktogramme und Texte können verändert werden. Sie können eine individuelle grafische Oberfläche für das Programm erstellen und es in einer anderen Sprache lokalisieren.

Gehen Sie folgendermaßen vor, um eine andere grafische Oberfläche zu verwenden:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Ansicht**.
3. Aktivieren Sie auf der rechten Fensterseite Grafische Oberflächen das Kontrollkästchen **Alternative Programmoberfläche verwenden**, um eine grafische Oberfläche einzubinden. Geben Sie im Eingabefeld den Ordner mit den Einstellungen der grafischen Oberfläche an oder klicken Sie auf **Durchsuchen**, um diesen Ordner zu suchen.

AKTIVE ELEMENTE DER BENUTZEROBERFLÄCHE

Sie können die Anzeige von aktiven Elementen der Benutzeroberfläche anpassen: z.B. Meldungsfenster, Symbol von Kaspersky Internet Security im Infobereich der Taskleiste.

Gehen Sie folgendermaßen vor, um die aktiven Elemente der Benutzeroberfläche anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Ansicht**.
3. Aktivieren oder deaktivieren Sie im Block **Symbol in der Taskleiste** die entsprechenden Kontrollkästchen

NEWS AGENT

Mit Hilfe von *News Agent* werden Sie von Kaspersky Lab über alle wichtigen Ereignisse informiert, die mit Kaspersky Internet Security und generell mit dem Schutz vor Computerbedrohungen zusammenhängen.

Wenn neue Nachrichten eintreffen, werden Sie vom Programm durch eine Popupmeldung im Infobereich der Taskleiste benachrichtigt. In diesem Fall verändert sich das Aussehen des Symbols (s. unten). Außerdem wird die Anzahl der ungelesenen Nachrichten im Programmhauptfenster genannt. Im Kontextmenü des Programmsymbols wird der Punkt **Nachrichten** angezeigt, und im Gadget für Kaspersky Internet Security erscheint das News-Symbol.

Die Nachrichten können folgendermaßen gelesen werden:

- Klicken Sie im Infobereich der Taskleiste auf das Symbol .
- Wählen Sie im Kontextmenü des Programmsymbols den Punkt **Neuigkeiten**.
- Klicken Sie in der News-Popupmeldung auf den Link **Nachrichten lesen**.
- Verwenden Sie den Link **Neuigkeiten** im Programmhauptfenster.
- Klicken Sie auf das Symbol , das in der Mitte des Gadgets erscheint, wenn Nachrichten verfügbar sind (nur für die Betriebssysteme Microsoft Windows Vista und Microsoft Windows 7).

Die aufgezählten Methoden zum Öffnen des Fensters von News Agent sind nur verfügbar, wenn ungelesene Nachrichten vorliegen.

Wenn Sie keine Nachrichten empfangen möchten, können Sie den Empfang von Nachrichten folgendermaßen

deaktivieren:

- aus dem Fenster von News Agent (nur verfügbar, wenn ungelesene Nachrichten vorliegen).
- aus dem Konfigurationsfensters des Programms.

Gehen Sie folgendermaßen vor, um den Empfang von Nachrichten aus dem Fenster von News Agent zu deaktivieren:

1. Öffnen Sie das Fenster von News Agent (siehe oben).
2. Deaktivieren Sie das Kontrollkästchen **Newsletter abonnieren**.

Gehen Sie folgendermaßen vor, um den Empfang von Nachrichten aus dem Programmkonfigurationsfenster zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Ansicht**.
3. Deaktivieren Sie im Block **Symbol in der Taskleiste** das Kontrollkästchen **Über Neuigkeiten benachrichtigen**.

MELDUNGEN

Standardmäßig werden Sie beim Auftreten von Ereignissen während der Ausführung von Kaspersky Internet Security entsprechend informiert. Wenn Sie über das weitere Vorgehen entscheiden sollen, erscheinen auf dem Bildschirm Meldungsfenster (s. Abschnitt "Meldungsfenster und Popupmeldungen" auf S. 50). Über Ereignisse, die keine Auswahl des weiteren Vorgehens erfordern, informiert das Programm mit Hilfe von akustischen Signalen, E-Mails und Popupmeldungen im Infobereich der Taskleiste (s. Abschnitt "Meldungsfenster und Popupmeldungen" auf S. 50).

Sie können für die Ereignisse eine Benachrichtigungsmethode (s. Abschnitt "Benachrichtigungsmethode anpassen" auf S. 200) wählen oder das Senden von Benachrichtigungen (s. Abschnitt "Benachrichtigungen aktivieren und deaktivieren" auf S. 199).

IN DIESEM ABSCHNITT

Benachrichtigungen aktivieren und deaktivieren 199

Benachrichtigungsmethode anpassen 200

BENACHRICHTIGUNGEN AKTIVIEREN UND DEAKTIVIEREN

Standardmäßig benachrichtigt Sie Kaspersky Internet Security auf verschiedene Arten über wichtige Ereignisse im Zusammenhang mit der Ausführung des Programms (s. Abschnitt "Benachrichtigungsmethode anpassen" auf S. 200). Sie können das Senden von Benachrichtigungen deaktivieren.

Die Informationen über Ereignisse, die während der Ausführung von Kaspersky Internet Security auftreten, werden unabhängig davon, ob die Benachrichtigungen aktiviert oder deaktiviert sind, im Bericht über die Programmarbeit protokolliert.

Die Deaktivierung der Benachrichtigungen hat keinen Einfluss auf die Anzeige der Meldungsfenster. Um nur eine minimale Anzahl an Meldungsfenstern auf dem Bildschirm anzeigen zu lassen, verwenden Sie den automatischen Schutzmodus (s. Abschnitt "Schutzmodus auswählen" auf S. 83).

Gehen Sie folgendermaßen vor, um das Senden von Meldungen zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Meldungen**.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Ereignisse melden**.

BENACHRICHTIGUNGSMETHODE ANPASSEN

Das Programm informiert Sie auf folgende Arten über Ereignisse:

- durch Popupmeldungen im Infobereich der Taskleiste;
- durch ein akustisches Signal;
- per E-Mail.

Die können die Benachrichtigungsmethoden für jede Art von Ereignis individuell einstellen.

Kritische Meldungen und Meldungen über Störungen des Programms werden standardmäßig von akustischen Signalen begleitet. Für die Audiosignale wird das Soundschema Microsoft Windows verwendet. Sie können ein anderes Schema wählen oder die Tonsignale ausschalten.

Gehen Sie wie folgt vor, um die Benachrichtigungsmethoden für die verschiedenen Ereignistypen zu konfigurieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Meldungen**.
3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Ereignisse melden** und klicken Sie auf die unterhalb des Kontrollkästchens angeordnete Schaltfläche **Einstellungen**.
4. Aktivieren Sie im erscheinenden Fenster **Meldungen** die Kontrollkästchen je nachdem, wie Sie Ihre Benachrichtigungen über die verschiedenen Ereignisse erhalten möchten: per E-Mail, in Form von Popupmeldungen oder per akustischem Signal. Um für einen bestimmten Ereignistyp keinerlei Benachrichtigungen zu erhalten, müssen Sie alle Kontrollkästchen in der Zeile dieses Ereignisses deaktivieren.

   Damit Kaspersky Internet Security Sie per E-Mail über Ereignisse benachrichtigen kann, müssen Sie die entsprechenden Einstellungen für die Zustellung per E-Mail vornehmen.

Gehen Sie folgendermaßen vor, um die E-Mail-Parameter für das Senden von Meldungen anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Meldungen**.
3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **E-Mails über Ereignisse senden** und klicken Sie auf **Einstellungen**.
4. Geben Sie im folgenden Fenster **E-Mail-Meldungen anpassen** die Versandparameter an.

Gehen Sie folgendermaßen vor, um das Soundschema zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Meldungen**.
3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Standardsoundschema Windows Default verwenden** und das vom Betriebssystem verwendete Schema.

Wenn das Kontrollkästchen deaktiviert ist, wird das Soundschema der vorhergehenden Programmversion verwendet.

Gehen Sie folgendermaßen vor, um die Audiosignale zur Begleitung von Benachrichtigungen zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Meldungen**.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Audiosignale für Meldungen aktivieren**.

TEILNAHME AN KASPERSKY SECURITY NETWORK

Jeden Tag taucht eine Vielzahl neuer Bedrohungen auf. Um ein schnelles Sammeln von Informationen über die Typen und Quellen neuer Bedrohungen zu gewährleisten und die Entwicklung entsprechender Neutralisierungsmethoden zu beschleunigen, können Sie sich dem Kaspersky Security Network anschließen.

Kaspersky Security Network (KSN) ist eine Infrastruktur der Online-Dienste und -Services, die den Zugriff auf die aktuelle Wissensdatenbank von Kaspersky Lab über den "Ruf" der Dateien, Internet-Ressourcen und Programme bietet. Durch die Verwendung der Daten von Kaspersky Security Network wird die Geschwindigkeit der Reaktion von Kaspersky Internet Security auf neue Bedrohungen und die Leistungsfähigkeit einiger Komponenten erhöht. Außerdem wird dadurch das Risiko verringert, dass Fehlalarme auftreten.

Bei Teilnahme am Kaspersky Security Network wird eine bestimmte Statistik, die während der Ausführung von Kaspersky Internet Security auf Ihrem Computer erstellt wird, automatisch an Kaspersky Lab übermittelt.

Es werden keine persönlichen Daten gesammelt, verarbeitet oder gespeichert.

Die Teilnahme an Kaspersky Security Network ist freiwillig. In der Regel entscheiden Sie im Verlauf der Installation von Kaspersky Internet Security über die Teilnahme. Allerdings können Sie Ihre Entscheidung jederzeit ändern.

Gehen Sie folgendermaßen vor, um die Verwendung von Kaspersky Security Network zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Feedback**.
3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Ich akzeptiere die Teilnahmebedingungen für Kaspersky Security Network**.

EINSTELLUNGEN VON KASPERSKY INTERNET SECURITY AUF KORREKTHEIT PRÜFEN

Nach der Installation und Konfiguration von Kaspersky Internet Security können Sie mit Hilfe eines "Testvirus" und dessen Modifikationen prüfen, ob die Einstellungen korrekt sind. Die Prüfung muss für jede Schutzkomponente und für jedes Protokoll einzeln ausgeführt werden.

In diesem Abschnitt

EICAR-"Testvirus" und seine Modifikationen 202

Testen des Schutzes für HTTP-Datenverkehr..... 204

Schutz für den SMTP-Datenverkehr testen..... 204

Überprüfung der Einstellungen von Datei-Anti-Virus..... 204

Überprüfung der Einstellungen für eine Aufgabe zur Virensuche..... 205

Überprüfung der Einstellungen für den Schutz vor unerwünschten E-Mails..... 205

EICAR-"Testvirus" und seine Modifikationen

Dieser "Testvirus" wurde vom Institut EICAR (The European Institute for Computer Antivirus Research) speziell zum Überprüfen der Arbeit von Antiviren-Produkten entwickelt.

Der Testvirus IST KEINE Schadsoftware und enthält keinen Programmcode, der Ihrem Computer Schaden zuzufügen könnte. Dennoch wird EICAR von den meisten Produkten der Entwickler von Virenschutzsoftware als Virus erkannt.

Verwenden Sie nie echte Viren, um die Funktionsfähigkeit eines Antiviren-Produkts zu testen!

Der "Testvirus" kann von der offiziellen Internetseite des EICAR-Instituts heruntergeladen werden: http://www.eicar.org/anti_virus_test_file.htm.

Vor dem Download muss der Viren-Schutz deaktiviert werden (s. Abschnitt "Schutz anhalten und fortsetzen" auf S. 58), weil der von der Seite anti_virus_test_file.htm heruntergeladene Testvirus andernfalls als infiziert erkannt und vom Programm als infiziertes, per HTTP-Protokoll übertragenes Objekt behandelt wird.

Die von der Webseite des EICAR-Instituts heruntergeladene Datei wird vom Programm als infiziertes Objekt identifiziert, das einen Virus enthält, der nicht desinfiziert werden kann, und führt die für diesen Objekttyp festgelegte Aktion aus.

Um die Funktion des Programms zu prüfen, können Sie auch Modifikationen des standardmäßigen "Testvirus" verwenden. Dazu wird der Inhalt des standardmäßigen "Testvirus" durch das Hinzufügen eines bestimmten Präfixes geändert (siehe Tabelle unten). Zum Erstellen von Modifikationen des "Testvirus" eignet sich ein beliebiger Text-Editor oder Hypertext-Editor wie beispielsweise Microsoft Editor, UltraEdit32, usw.

Die erste Spalte der Tabelle (s. unten) enthält Präfixe, die dem Standard-Testvirus zur Erzeugung einer Modifikation am Zeilenanfang hinzugefügt werden müssen. Die zweite Spalte zeigt die möglichen Werte für den Status, der einem Objekt aufgrund der Untersuchungsergebnisse zugewiesen werden kann. Die dritte Spalte bietet Informationen darüber, wie

Objekte mit dem betreffenden Status vom Programm bearbeitet werden. Beachten Sie, dass die Aktionen für Objekte durch die Werte der Programmparameter bestimmt werden.

Nach Hinzufügen des Präfixes zum Testvirus speichern Sie die so entstandene Datei unter einem Namen, der eine Vorstellung von der Modifikationen des Virus vermittelt: Wenn Sie beispielsweise das Präfix DELE- hinzugefügt haben, bietet es sich an, die entstandene Datei unter dem Namen eicar_dele.com zu speichern.

Vergessen Sie nicht, den Virenschutz nach dem Download des Testvirus und der Herstellung der Modifikationen zu aktualisieren.

Tabelle 2. Modifikationen des "Testvirus"

Präfix	Status des Objekts	Informationen zur Verarbeitung des Objekts
Kein Präfix, standardmäßiger "Testvirus".	**Infiziert**. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Programm identifiziert dieses Objekt als Virus, der nicht desinfiziert werden kann. Beim Desinfektionsversuch des Objekts tritt ein Fehler auf und die für irreparable Objekte geltende Aktion wird ausgeführt.
CORR-	**Beschädigt**.	Das Programm hat Zugriff auf das Objekt erhalten, kann es aber aufgrund einer Beschädigung nicht untersuchen (z.B. beschädigte Struktur des Objekts, ungültiges Dateiformat). Informationen darüber, dass das Objekt verarbeitet wurde, können Sie dem Bericht über die Arbeit der Anwendung entnehmen.
WARN-	**Verdächtig**. Das Objekt enthält einen unbekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Objekt wurde als verdächtig erkannt. Im Augenblick des Funds enthalten die Programm-Datenbanken keine Beschreibung zur Desinfektion dieses Objekts. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
SUSP-	**Verdächtig**. Das Objekt enthält den modifizierten Code eines bekannten Virus. Die Desinfektion ist nicht möglich.	Das Programm hat erkannt, dass der Objektcode teilweise mit dem Code eines bekannten Virus übereinstimmt. Im Augenblick des Funds enthalten die Programm-Datenbanken keine Beschreibung zur Desinfektion dieses Objekts. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
ERRO-	**Untersuchungsfehler**.	Bei der Untersuchung des Objekts ist ein Fehler aufgetreten. Die Anwendung erhielt keinen Zugriff auf das Objekt: Die Integrität des Objekts ist beschädigt (z.B. kein Endpunkt in einem Multi-Level-Archiv) oder die Verbindung zu dem Objekt fehlt (wenn ein Objekt in einer Netzwerkressource untersucht wird). Informationen darüber, dass das Objekt verarbeitet wurde, können Sie dem Bericht über die Arbeit der Anwendung entnehmen.
CURE-	**Infiziert**. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist möglich.	Das Objekt enthält einen Virus, der desinfiziert werden kann. Das Programm führt die Desinfektion des Objekts aus, wobei der Text des Viruskörpers in CURE geändert wird. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.
DELE-	**Infiziert**. Das Objekt enthält einen bekannten Viruscode. Die Desinfektion ist nicht möglich.	Das Programm identifiziert dieses Objekt als Virus, der nicht desinfiziert werden kann. Beim Desinfektionsversuch des Objekts tritt ein Fehler auf und die für irreparable Objekte geltende Aktion wird ausgeführt. Beim Fund eines solchen Objekts, erhalten Sie eine Meldung.

TESTEN DES SCHUTZES FÜR HTTP-DATENVERKEHR

Gehen Sie folgendermaßen vor, um die den Virenschutz für den mit HTTP-Protokoll übertragenen Datenverkehr zu prüfen:

Versuchen Sie, den "Testvirus" von der offiziellen Internetseite des **EICAR**-Instituts herunterzuladen: http://www.eicar.org/anti_virus_test_file.htm.

Beim Versuch, den "Testvirus" herunterzuladen, erkennt Kaspersky Internet Security das Objekt, identifiziert es als infiziert und irreparabel, und führt die Aktion aus, die in den Einstellungen für die Untersuchung des HTTP-Datenverkehrs dafür festgelegt wurde. Wenn versucht wird, den "Testvirus" herunterzuladen, wird in der Grundeinstellung die Verbindung mit der Ressource getrennt und im Browserfenster erscheint eine Meldung darüber, dass dieses Objekt von dem Virus EICAR-Test-File infiziert ist.

SCHUTZ FÜR DEN SMTP-DATENVERKEHR TESTEN

Um den Virenschutz für den mit SMTP-Protokoll übertragenen Datenverkehr zu prüfen, können Sie ein Mailprogramm verwenden, das die Daten mit diesem Protokoll überträgt.

Es wird empfohlen, die Virenerkennung in verschiedenen Teilen ausgehender Nachrichten zu testen, sowohl im Nachrichtenkörper als auch in den Anlagen. Verwenden Sie zu Testzwecken die Datei des EICAR-Testvirus (s. Abschnitt "EICAR-"Testvirus" und seine Modifikationen" auf S. 202).

Zum Testen der Virenerkennung in einem per SMTP-Protokoll versandten Datenstrom gehen Sie wie folgt vor:

1. Erstellen Sie mit Hilfe des auf Ihrem Computer installierten Mailprogramms eine E-Mail im Format Gewöhnlicher Text.

   Eine Nachricht, die den "Testvirus" enthält und das Format RTF oder HTML besitzt, wird nicht untersucht!

2. Führen Sie abhängig davon, in welchem Teil der Nachricht der Virus gefunden werden soll, folgende Aktionen aus:

   - Fügen Sie für den Fund des Virus im Nachrichtenkörper den Text des Standard-EICAR-Testvirus oder eines modifizierten EICAR-Testvirus am Anfang der Nachricht ein.
   - Für einen Virenfund in den Anhängen hängen Sie an die Nachricht eine Datei mit dem EICAR-Testvirus an.

3. Schicken Sie die E-Mail an die Adresse des Administrators.

Das Programm erkennt das Objekt, identifiziert es als infiziert und blockiert das Senden der E-Mail.

ÜBERPRÜFUNG DER EINSTELLUNGEN VON DATEI-ANTI-VIRUS

Gehen Sie folgendermaßen vor, um zu prüfen, ob Datei-Anti-Virus korrekt eingestellt wurde:

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen Seite des **EICAR**-Instituts (http://www.eicar.org/anti_virus_test_file.htm) heruntergeladenen Testvirus und die von Ihnen erstellten Modifikationen des Testvirus in diesen Ordner.

2. Erlauben Sie das Protokollieren aller Ereignisse, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht werden, in der Berichtsdatei gespeichert werden.

3. Starten Sie den "Testvirus" oder seine Modifikation zur Ausführung.

Datei-Anti-Virus fängt den Zugriff auf die Datei ab, untersucht sie und führt die in den Einstellungen festgelegte Aktion aus. Durch die Auswahl unterschiedlicher Aktionsvarianten für ein gefundenes Objekt können Sie die Funktion der Komponente vollständig testen.

Vollständige Informationen über die Arbeitsergebnisse von Datei-Anti-Virus sind im Bericht über die Arbeit der Komponente enthalten.

ÜBERPRÜFUNG DER EINSTELLUNGEN FÜR EINE AUFGABE ZUR VIRENSUCHE

Gehen Sie folgendermaßen vor, um zu prüfen, ob eine Aufgabe zur Virensuche korrekt eingestellt wurde:

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen Seite des **EICAR**-Instituts (http://www.eicar.org/anti_virus_test_file.htm) heruntergeladenen Testvirus und die von Ihnen erstellten Modifikationen des Testvirus in diesen Ordner.

2. Erstellen Sie eine neue Untersuchungsaufgabe und wählen Sie als Untersuchungsobjekt den Ordner, der die "Testviren" enthält.

3. Erlauben Sie das Protokollieren aller Ereignisse, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht werden, in der Berichtsdatei gespeichert werden.

4. Starten Sie die Ausführung der Untersuchungsaufgabe.

Wenn bei der Untersuchung verdächtige oder infizierte Objekte gefunden werden, werden die in den Einstellungen der Aufgabe festgelegten Aktionen ausgeführt. Durch die Auswahl unterschiedlicher Aktionsvarianten für ein gefundenes Objekt können Sie die Funktion der Komponente vollständig testen.

Vollständige Informationen über das Ausführungsergebnis der Untersuchungsaufgabe sind im Bericht über die Arbeit der Komponente enthalten.

ÜBERPRÜFUNG DER EINSTELLUNGEN FÜR DEN SCHUTZ VOR UNERWÜNSCHTEN E-MAILS

Zur Überprüfung des Schutzes vor unerwünschten E-Mails können Sie eine Testnachricht verwenden, die vom Programm als Spam identifiziert wird.

Die Testnachricht muss folgenden Text in der Betreffzeile enthalten:

```
Spam is bad do not send it
```

Nachdem diese Nachricht auf dem Computer eingetroffen ist, untersucht Kaspersky Internet Security sie, stuft sie als Spam ein und führt die Aktion damit aus, die für diesen Objekttyp festgelegt wurde.

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Wenn bei der Verwendung von Kaspersky Internet Security Probleme auftreten sollten, prüfen Sie zuerst, ob die Dokumentation, die Hilfe, die Wissensdatenbank auf der Seite des Technischen Supports von Kaspersky Lab oder das Benutzerforum keine Lösung dafür bieten.

Wenn Sie keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support von Kaspersky Lab. Dies ist auf folgende Weise möglich:

- aus Mein Kaspersky Account eine Anfrage an die Webseite des Technischen Supports senden.
- telefonisch

Die Spezialisten des Technischen Supports beantworten Ihre Fragen zur Installation, Aktivierung und Verwendung des Programms. Wenn Ihr Computer infiziert wurde, helfen sie Ihnen dabei, die Folgen der schädlichen Malware-Aktionen zu beheben.

Bevor Sie sich an den technischen Support wenden, lesen Sie sich bitte zuvor die Supportrichtlinien (http://support.kaspersky.de/support/rules) durch.

Wenn Sie sich an den Technischen Support wenden, bitten die Support-Experten Sie möglicherweise darum, einen Bericht über den Systemzustand und eine Protokolldatei zu erstellen und diese an den Technischen Support zu senden. Aufgrund einer Analyse der von Ihnen eingesandten Daten können die Support-Experten ein AVZ-Skript erstellen, das an Sie geschickt wird. Mit diesem Skript können Sie die aufgetretenen Probleme beheben.

In diesem Abschnitt

Mein Kaspersky Account 206

Technischer Support am Telefon 207

Bericht über den Systemzustand erstellen 207

Protokolldatei erstellen 208

Dateien mit Daten senden 208

AVZ-Skript ausführen 209

MEIN KASPERSKY ACCOUNT

Mein Kaspersky Account ist Ihr persönlicher Bereich auf der Seite des Technischen Supports. Dort können Sie folgende Aktionen ausführen:

- Anfragen an den Technischen Support und an das Virenlabor senden.
- ohne E-Mail mit dem Technischen Support kommunizieren.
- Status Ihrer Anfragen in Echtzeit verfolgen.
- Verlauf Ihrer Zugriffe auf den Technischen Support ansehen.

Verwenden Sie eine der folgenden Methoden, um die Login-Seite für den persönlichen Bereich zu öffnen:

- Verwenden Sie den Link **Mein Kaspersky Account** im Hauptfenster von Kaspersky Internet Security.
- Geben Sie in der Adressenleiste des Browsers ein: .

Wenn Sie noch keinen Kaspersky Account besitzen, können Sie auf die Registrierungsseite https://my.kaspersky.com/de/registration gehen. Geben Sie hier Ihre E-Mail-Adresse und ein Kennwort für den Zugriff auf Ihren Kaspersky Account an. Für Anfragen zu Kaspersky Internet Security benötigen Sie den Aktivierungscode des Programms.

Beachten Sie, dass bestimmte Anfragen nicht an den Technischen Support, sondern an das Virenlabor gerichtet werden müssen. Dazu zählen folgende Arten von Anfragen:

- Unbekanntes Schadprogramm – Sie haben den Verdacht, dass ein bestimmtes Objekt schädlich ist, obwohl Kaspersky Internet Security es nicht als Malware einstuft.
- Viren-Fehlalarm – Kaspersky Internet Security stuft eine bestimmte Datei als infiziert ein, während Sie sicher sind, dass die Datei virenfrei ist.
- Anfrage für eine Beschreibung eines Schadprogramms – Sie möchten die Beschreibung eines bestimmten Virus erhalten.

Für Anfragen an das Virenlabor ist kein Aktivierungscode erforderlich.

Anfragen an das Virenlabor können Sie auf der Seite (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de) stellen.

TECHNISCHER SUPPORT AM TELEFON

Zur Lösung dringender Probleme können Sie jederzeit Ihren lokalen Technischen Support anrufen. Bevor Sie sich an die Fachleute vom deutschsprachigen oder internationalen technischen Support wenden, tragen Sie bitte Daten über Ihren Computer und das installierte Antiviren-Produkt zusammen. Dadurch können unsere Spezialisten Ihnen möglichst schnell helfen.

BERICHT ÜBER DEN SYSTEMZUSTAND ERSTELLEN

Damit die Support-Spezialisten von Kaspersky Lab Sie bei der Lösung eines Problems unterstützen können, kann es erforderlich sein, einen Bericht über den Zustand des Systems zu erstellen. Dieser Bericht enthält ausführliche Informationen über gestartete Prozesse, geladene Module und Treiber, Erweiterungsmodule für Microsoft Internet Explorer und Microsoft Windows Explorer, offene Ports, gefundene verdächtige Objekte u.a.

Beim Erstellen des Berichts über den Systemzustand werden keine persönlichen Benutzerdaten gesammelt.

Gehen Sie folgendermaßen vor, um einen Bericht über den Systemzustand zu erstellen:

1. Öffnen Sie das Programmhauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security " auf S. 47).
2. Klicken Sie im unteren Bereich des Hauptfensters auf **Support**, um das Fenster **Support** zu öffnen, und klicken Sie dort auf den Link **Protokollierung**.
3. Klicken Sie im folgenden Fenster **Informationen für den Support** auf **Bericht über den Systemstatus erstellen**.

Der Bericht über den Systemzustand wird in den Formaten html und xml erstellt und im Archiv sysinfo.zip gespeichert. Nachdem das Sammeln von Daten über das System abgeschlossen wurde, können Sie einen Bericht ansehen.

Gehen Sie folgendermaßen vor, um einen Bericht anzuzeigen:

1. Öffnen Sie das Programmhauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security " auf S. 47).
2. Klicken Sie im unteren Bereich des Hauptfensters auf **Support**, um das Fenster **Support** zu öffnen, und klicken Sie dort auf den Link **Protokollierung**.
3. Klicken Sie im folgenden Fenster **Informationen für den Support** auf **Anzeigen**.
4. Öffnen Sie das Archiv sysinfo.zip, das die Protokolldateien enthält.

PROTOKOLLDATEI ERSTELLEN

Nach der Installation von Kaspersky Internet Security können bei der Arbeit des Betriebssystems oder bestimmter Programme Störungen auftreten. Dies deutet höchstwahrscheinlich auf einen Konflikt von Kaspersky Internet Security mit einem Programm, das auf Ihrem Computer installiert ist, oder mit auf Ihrem Computer vorhandenen Treibern hin. Damit die Support-Spezialisten von Kaspersky Lab Sie bei der Lösung Ihres Problems unterstützen können, kann es sein, dass der Support Sie auffordert, eine Protokolldatei zu erstellen.

Gehen Sie folgendermaßen vor, um eine Protokolldatei zu erstellen:

1. Öffnen Sie das Programmhauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security " auf S. 47).
2. Klicken Sie im unteren Bereich des Hauptfensters auf **Support**, um das Fenster **Support** zu öffnen, und klicken Sie dort auf den Link **Protokollierung**.
3. Wählen Sie im folgenden Fenster **Informationen für den Support** unter **Protokollierung** aus der Dropdown-Liste ein Protokollierungsniveau.

   Es wird empfohlen, die Support-Experten nach dem erforderlichen Tracing-Niveau zu fragen. Sollte diese Angabe des Supports fehlen, dann empfohlen, das Tracing-Niveau **500** einzustellen.
4. Klicken Sie auf **Aktivieren**, um den Protokollierungsvorgang zu starten.
5. Wiederholen Sie die Situation, in der das Problem aufgetreten ist.
6. Klicken Sie auf **Deaktivieren**, um den Protokollierungsvorgang zu beenden.

Sie können mit dem Hochladen der Protokollierungsergebnisse (s. Abschnitt "Datendateien versenden" auf S. 208) auf den Server von Kaspersky Lab beginnen.

DATEIEN MIT DATEN SENDEN

Nachdem die Protokolldateien und der Bericht über den Systemzustand erstellt wurden, müssen diese an den Technischen Support von Kaspersky Lab geschickt werden.

Um die Dateien mit den Daten auf den Server des Technischen Supports hochzuladen, benötigen Sie eine Anfragenummer. Diese Nummer erhalten Sie in Ihrem Kaspersky Account auf der Webseite des Technischen Supports, wenn eine aktive Anfrage vorliegt.

Gehen Sie folgendermaßen vor, um die Dateien mit den Daten auf den Server des Technischen Supports hochzuladen:

1. Öffnen Sie das Programmhauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security " auf S. 47).
2. Klicken Sie im unteren Bereich des Hauptfensters auf **Support**, um das Fenster **Support** zu öffnen, und klicken Sie dort auf den Link **Protokollierung**.

3. Klicken Sie im folgenden Fenster **Informationen für den Support** im Block **Aktionen** auf **Informationen für den Support auf den Server laden**.

   Das Fenster **Support-Informationen auf Server hochladen** wird geöffnet.

4. Aktivieren Sie die Kontrollkästchen neben den Dateien, die Sie an den Technischen Support schicken möchten, und klicken Sie auf **Senden**.

   Das Fenster **Anfragenummer** wird geöffnet.

5. Geben Sie die Nummer an, die Ihre Anfrage in Mein Kaspersky Account vom Technischen Support erhalten hat, und klicken Sie auf **OK**.

Die gewählten Dateien werden komprimiert und an den Server des Technischen Supports gesendet.

Falls kein Kontakt mit dem Technischen Support möglich ist, können Sie diese Dateien auf Ihrem Computer speichern und sie später aus Mein Kaspersky Account absenden.

Gehen Sie folgendermaßen vor, um die Dateien mit Daten auf der Festplatte zu speichern:

1. Öffnen Sie das Programmhauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security " auf S. 47).

2. Klicken Sie im unteren Bereich des Hauptfensters auf **Support**, um das Fenster **Support** zu öffnen, und klicken Sie dort auf den Link **Protokollierung**.

3. Klicken Sie im folgenden Fenster **Informationen für den Support** im Block **Aktionen** auf **Informationen für den Support auf den Server laden**.

   Das Fenster **Support-Informationen auf Server hochladen** wird geöffnet.

4. Aktivieren Sie die Kontrollkästchen neben den Dateien, die Sie an den Technischen Support schicken möchten, und klicken Sie auf **Senden**.

   Das Fenster **Anfragenummer** wird geöffnet.

5. Klicken Sie auf **Abbrechen** und bestätigen Sie im folgenden Fenster mit **Ja**, dass die Dateien auf der Festplatte gespeichert werden.

   Ein Fenster zum Speichern des Archivs wird geöffnet.

6. Geben Sie einen Namen für das Archiv an und bestätigen Sie das Speichern.

Das fertige Archiv können Sie über Mein Kaspersky Account an den Technischen Support senden.

AVZ-SKRIPT AUSFÜHREN

Die Spezialisten von Kaspersky Lab analysieren Ihr Problem auf der Grundlage von Protokolldateien und eines Berichts über den Systemzustand. Das Ergebnis der Analyse besteht aus einer Reihe von Aktionen, die dazu dienen, die gefundenen Probleme zu beheben. Oft handelt es sich dabei um sehr viele Aktionen.

Um die Problembehebung zu vereinfachen, werden AVZ-Skripts verwendet. Ein AVZ-Skript ist eine Kombination von Befehlen, die es erlauben, Registrierungsschlüssel zu ändern, Dateien in die Quarantäne zu verschieben, eine Klassensuche mit der Möglichkeit der Isolierung von damit verbundenen Dateien vorzunehmen, Hooks der Typen UserMode und KernelMode zu blockieren, u.a.

Zum Starten der Skripts bietet das Programm einen *Assistenten zum Ausführen von AVZ-Skripts*.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Es wird davor gewarnt, den Text eines Skripts, das Ihnen von den Support-Spezialisten geschickt wurde, zu verändern. Sollten bei der Skript-Ausführung Probleme auftreten, dann wenden Sie sich an den Technischen Support.

Gehen Sie folgendermaßen vor, den Assistenten zu starten:

1. Öffnen Sie das Programmhauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security " auf S. 47).
2. Klicken Sie im unteren Bereich des Hauptfensters auf **Support**, um das Fenster **Support** zu öffnen, und klicken Sie dort auf den Link **Protokollierung**.
3. Klicken Sie im folgenden Fenster **Informationen für den Support** auf **AVZ-Skript ausführen**.

Wenn das Skript erfolgreich ausgeführt wurde, wird der Assistent abgeschlossen. Falls bei der Skript-Ausführung Störungen auftreten, zeigt der Assistent eine entsprechende Meldung an.

ANHÄNGE

Dieser Abschnitt enthält Hilfeinformationen, die den Haupttext des Dokuments ergänzen.

IN DIESEM ABSCHNITT

Varianten für den Abo-Status 211

Liste der Benachrichtigungen von Kaspersky Internet Security 213

Bedienung des Programms über die Befehlszeile 231

VARIANTEN FÜR DEN ABO-STATUS

Es bestehen folgende Varianten für den Abonnementstatus:

- *wird ermittelt*. Die Anfrage auf Aktivierung des Abonnements wurde noch nicht verarbeitet (für die Verarbeitung der Anfrage wird auf dem Server eine bestimmte Zeit benötigt). Kaspersky Internet Security arbeitet im vollfunktionalen Modus. Wenn die Abonnementanfrage nach Ablauf eines bestimmten Zeitraums nicht verarbeitet wurde, werden Sie darüber benachrichtigt, dass der Abonnementstatus nicht aktualisiert ist. Gleichzeitig werden die Programm-Datenbanken nicht mehr aktualisiert (für eine Lizenz mit Update-Abonnement) und der Computerschutz wird beendet (für eine Lizenz mit Update- und Schutz-Abonnement).

- *wurde aktiviert*. Das Abonnement wurde unbegrenzt oder für einen bestimmten Zeitraum aktiviert (festes Ablaufdatum des Abonnements).

- *wurde verlängert*. Das Abonnement wurde unbegrenzt oder für einen bestimmten Zeitraum verlängert.

- *Fehler*. Bei Aktualisierung des Abonnementstatus ist ein Fehler aufgetreten.

- *ist abgelaufen. Ihnen wird eine Ermässigung gewährt.* Die Gültigkeit des Abonnements oder der Zeitraum, während dem der Abonnementstatus aktualisiert werden muss, ist abgelaufen. Wenn der Zeitraum, während dem der Abonnementstatus aktualisiert werden muss, abgelaufen ist, aktualisieren Sie den Abonnementstatus manuell. Wenn die Gültigkeit des Abonnements abgelaufen ist, können Sie das Abonnement verlängern. Wenden Sie sich dazu an den Online-Shop, bei dem Sie Kaspersky Internet Security erworben haben. Um einen anderen Aktivierungscode zu verwenden, löschen Sie die Schlüsseldatei des verwendeten Abonnements.

- *ist abgelaufen. Die Ermässigungsfrist ist abgelaufen.* Die Gültigkeit des Abonnements oder die Ermäßigungsfrist für Lizenzverlängerung ist abgelaufen. Wenden Sie sich an den Lieferanten des Abonnements, um ein neues Abonnement zu kaufen oder das vorhandene Abonnement zu aktualisieren.

  Wenn die Gültigkeit des Abonnements abgelaufen und die Ermäßigungsfrist, in der eine Verlängerung möglich war, verstrichen ist (Abo-Status – *Abgelaufen*), benachrichtigt Kaspersky Internet Security Sie darüber und versucht nicht mehr, das Abonnement automatisch zu verlängern. Für eine Lizenz mit Update-Abonnement bleibt die Funktionalität des Programms unter Ausnahme des Updates der Programm-Datenbanken erhalten. Für eine Lizenz mit Update- und Schutz-Abonnement werden die Datenbanken des Programms nicht mehr aktualisiert, der Computerschutz wird eingestellt und die Untersuchungsaufgaben werden nicht mehr gestartet.

- *Das Abonnement wurde gekündigt*. Sie haben die Verwendung eines Abonnements zur automatischen Lizenzverlängerung verworfen.

- *Aktualisierung ist erforderlich*. Der Abonnementstatus wurde aus bestimmten Gründen nicht rechtzeitig aktualisiert.

  Wenn das Abonnement nicht rechtzeitig aktualisiert wurde (wenn beispielsweise der Computer während des gesamten Zeitraums ausgeschaltet war, in dem eine Lizenzverlängerung möglich war), können Sie den Abo-

Status im Fenster Lizenzverwaltung manuell aktualisieren (s. Abschnitt "Lizenz-Info anzeigen" auf S. 44). Bis zur Verlängerung des Abonnements lädt Kaspersky Internet Security keine Updates für die Programm-Datenbanken herunter (für eine Lizenz mit Update-Abonnement), stellt den Computerschutz ein und startet keine Untersuchungsaufgaben (für eine Lizenz mit Update- und Schutz-Abonnement).

- *wurde angehalten*. Abonnement zur automatischen Lizenzverlängerung wurde angehalten.
- *wurde erneuert*. Das Abonnement wurde aktualisiert.

In einigen Fällen können für eine Lizenz mit Abonnement zusätzliche Informationen zum Abo-Status angezeigt werden.

Liste der Benachrichtigungen von Kaspersky Internet Security

Dieser Abschnitt bietet eine Liste der Benachrichtigungen, die bei der Arbeit von Kaspersky Internet Security auf dem Bildschirm erscheinen können.

In diesem Abschnitt

Meldungen in allen Schutzmodi 213

Meldungen im interaktiven Schutzmodus 220

Meldungen in allen Schutzmodi

Dieser Abschnitt enthält alle Meldungen, die bei der Arbeit des Programms sowohl im automatischen als auch im interaktiven Schutzmodus erscheinen können (s. Abschnitt "Schutzmodus auswählen" auf S. 83). Wenn Sie alle verfügbaren Meldungen sehen möchten, schalten Sie zum interaktiven Schutzmodus um. Dann werden nicht nur die in diesem Abschnitt genannten Meldungen auf dem Bildschirm angezeigt, sondern auch jene, die nur im interaktiven Schutzmodus (s. Abschnitt "Meldungen im interaktiven Schutzmodus" auf S. 220) erscheinen.

In diesem Abschnitt

Spezielle Desinfektionsprozedur ist erforderlich 214

Verstecktes Laden eines Treibers 214

Ein Programm ohne digitale Signatur wird gestartet 215

Ein Wechseldatenträger wurde angeschlossen 215

Neues Netzwerk wurde gefunden 215

Ein unsicheres Zertifikat wurde gefunden 216

Erlaubnisanfrage für den Zugriff auf eine Webseite aus einer regionalen Domain 216

Ein potentiell gefährliches Programm wurde gefunden 217

In Quarantäne befindliche Datei ist nicht infiziert 217

Eine neue Produktversion ist erschienen 218

Ein technisches Update ist erschienen 218

Ein technisches Update wurde heruntergeladen 218

Das heruntergeladene technische Update wurde nicht installiert 219

Lizenz abgelaufen 219

SPEZIELLE DESINFEKTIONSPROZEDUR IST ERFORDERLICH

Beim Fund einer Bedrohung, die gerade im System aktiv ist (beispielsweise ein schädlicher Prozess im Arbeitsspeicher oder in den Autostart-Objekten), erscheint auf dem Bildschirm eine Meldung, die dazu auffordert, eine speziell dafür vorgesehene erweiterte Desinfektionsprozedur durchzuführen.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Art der Bedrohung und Name des schädlichen Objekts gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen eines schädlichen Objekts befindet sich das Symbol. Durch Klick auf das Symbol wird ein Fenster mit Informationen über das Objekt geöffnet. Aus diesem Fenster gelangen Sie über den Link www.securelist.com zur Webseite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen über die Bedrohung erhalten können, die dieses Objekt darstellt.
- Dateiname und Pfad eines schädlichen Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen zu wählen:

- **Ja, bei Neustart desinfizieren** – Spezielle Desinfektionsprozedur ausführen.

  Die Kaspersky-Lab-Experten empfehlen ausdrücklich, diese Variante zu wählen. Beachten Sie aber, dass zum Abschluss des Vorgangs das Betriebssystem neu gestartet wird. Deshalb sollten die aktuellen Arbeitsergebnisse gespeichert und alle Anwendungen geschlossen werden, bevor der Vorgang ausgeführt wird. Während des Desinfektionsvorgangs können nur vertrauenswürdige Programme gestartet werden, alle anderen werden blockiert. Nach dem Neustart des Computers wird empfohlen, die vollständige Virenuntersuchung zu starten.
- **Nicht ausführen** – Das gefundene Objekt oder der Prozess wird entsprechend der zuvor gewählten Aktion verarbeitet.

Aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**, damit die gewählte Aktion künftig immer in ähnlichen Situationen angewendet wird.

VERSTECKTES LADEN EINES TREIBERS

Bestimmte Schadprogramme laden heimlich Treiber auf einen PC. Anschließend lässt sich die Aktivität des Schadprogramms nicht mehr mit Kaspersky Internet Security kontrollieren. Diese Methode des Treiberdownloads wird nur selten von legalen Programmen verwendet.

Wenn die Programmkontrolle einen Versuch zum heimlichen Treiberdownload erkennt, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Name und Pfad der Treiberdatei

  Neben dem Dateinamen befindet sich das Symbol. Durch Klick auf das Symbol wird ein Fenster mit Informationen über den Treiber geöffnet.

Folgende Aktionen stehen zur Auswahl:

- **Jetzt erlauben** – Download des Treibers erlauben und Treiber zur Ausnahmeliste hinzufügen.
- **Jetzt verbieten** – Download des Treibers verbieten.
- **Quarantäne** – Download des Treibers verbieten und Treiberdatei in die Quarantäne verschieben.

EIN PROGRAMM OHNE DIGITALE SIGNATUR WIRD GESTARTET

Wenn die Programmkontrolle erkennt, dass auf dem Computer ein Programm gestartet wird, das keine digitale Signatur besitzt und das aufgrund einer heuristischen Analyse einen hohen Risikowert erhalten hat, so erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Name des zu startenden Programms

  Neben dem Namen des Programms befindet sich das Symbol . Durch Klick auf das Symbol wird ein Fenster mit Informationen über das Programm geöffnet.

- Angaben über die Anzahl der Benutzer, die das Programm verwenden und ihm vertrauen.

Sie können festlegen, ob Sie dem Programm vertrauen. Wählen Sie dazu eine der folgenden Aktionen:

- **Ja, ich vertraue** – Start und Ausführung des Programms uneingeschränkt erlauben.
- **Programm beschränken** – Start des Programms erlauben, aber die Ausführung gefährlicher Operationen verbieten.
- **Blockieren** – Start und Ausführung des Programms jetzt und künftig verbieten.

EIN WECHSELDATENTRÄGER WURDE ANGESCHLOSSEN

Wenn ein Wechseldatenträger an den Computer angeschlossen wird, erscheint eine Meldung auf dem Bildschirm. Ihnen wird angeboten, eine der folgenden Aktionen zu wählen:

- **Schnelle Untersuchung** – Nur jene Dateien auf dem Wechseldatenträger untersuchen, die ein potentielles Risiko darstellen können.
- **Vollständige Untersuchung** – Alle Dateien auf dem Wechseldatenträger untersuchen.
- **Nicht untersuchen** – Wechseldatenträger nicht untersuchen.

Aktivieren Sie das Kontrollkästchen **In ähnlichen Fällen immer anwenden**, damit die gewählte Aktion künftig auf alle verbundenen Wechseldatenträger angewendet wird.

NEUES NETZWERK WURDE GEFUNDEN

Bei jeder Verbindung des Computers mit einer neuen Zone (Netzwerk) erscheint eine Meldung auf dem Bildschirm.

Im oberen Bereich der Meldung werden Informationen zum Netzwerk genannt:

- Netzwerkadapter, der für die Netzwerkverbindung verwendet wird.
- Typ des Netzwerks (z.B. "drahtlos")
- Name des Netzwerks

Im unteren Teil können Sie einen Status für die gefundene Zone festlegen, auf dessen Grundlage entschieden wird, welche Art von Netzwerkaktivität erlaubt wird:

- **Ja, das ist ein vertrauenswürdiges Netzwerk**. Es wird empfohlen, diesen Status nur für absolut sichere Zonen zu verwenden, in denen dem Computer keine Angriffe und Versuche zum unerlaubten Datenzugriff drohen.
- **Lokales Netzwerk**. Es wird empfohlen, diesen Status für Zonen mit mittlerer Risikostufe anzuwenden (beispielsweise für interne Firmennetzwerk).
- **Nein, das ist ein öffentliches Netzwerk**. Netzwerk mit hoher Risikostufe. Bei der Arbeit in dieser Zone ist der Computer allen möglichen Typen von Bedrohungen ausgesetzt. Dieser Status wird auch für Netzwerke empfohlen, die nicht durch Antiviren-Programme, Firewalls, Filter usw. geschützt werden. Die Auswahl dieses Status gewährleistet dem Computer bei der Arbeit in dieser Zone maximale Sicherheit.

EIN UNSICHERES ZERTIFIKAT WURDE GEFUNDEN

Die Zuverlässigkeit einer SSL-Verbindung wird mit Hilfe des installierten Zertifikats geprüft. Wenn beim Verbindungsversuch mit einem Server ein inkorrektes Zertifikat verwendet wird (z.B. wenn es von einem Angreifer ausgetauscht wurde), erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Link für die Anzeige des Zertifikats
- Mögliche Fehlerursachen
- Webadresse der Ressource

Sie werden aufgefordert zu entscheiden, ob unter Verwendung des unsicheren Zertifikats eine Verbindung hergestellt werden soll:

- **Ja, unsicheres Zertifikat akzeptieren** – Verbindung mit der Webressource fortsetzen.
- **Zertifikat ablehnen** – Verbindung mit der Webressource trennen.

ERLAUBNISANFRAGE FÜR DEN ZUGRIFF AUF EINE WEBSEITE AUS EINER REGIONALEN DOMAIN

Beim Zugriff auf eine Webseite aus einer regionalen Domain, für die nicht festgelegt wurde, ob der Zugriff erlaubt oder verboten ist, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung des Grunds, aus dem der Zugriff auf die Webseite blockiert wurde.
- Name der Region, zu der die Webseite gehört.
- Domain und Beschreibung des Kontaminationsgrads der Webseiten in dieser Domain
- Adresse der Webseite
- Name des Programms, das den Zugriff auf die Webseite ausgeführt hat.

Folgende Aktionen stehen zur Auswahl:

- **Ja, Zugriff erlauben** – Webseite laden.

- **Nein, Zugriff verbieten** – Laden der Webseite verwerfen.

Aktivieren Sie das Kontrollkästchen **Für diese Region speichern**, damit die gewählte Aktion künftig auf alle Webseiten aus dieser regionalen Domain angewendet wird.

EIN POTENTIELL GEFÄHRLICHES PROGRAMM WURDE GEFUNDEN

Wenn der Aktivitätsmonitor ein Programm erkennt, dessen Verhalten Ähnlichkeit mit den Aktionen von Schadprogrammen besitzt, so erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Typ und Name des potentiell gefährlichen Programms

  Neben dem Namen des Programms befindet sich das Symbol . Durch Klick auf das Symbol wird ein Fenster mit Informationen über das Programm geöffnet.
- Prozess-ID, Name und Pfad der Programmdatei.
- Dieser Link führt zum Fenster mit einem Ereignisverlauf für das Programm.

Folgende Aktionen stehen zur Auswahl:

- **Quarantäne** – Programm beenden und Programmdatei in die Quarantäne verschieben, wo sie keine Gefahr für Ihren Computer darstellt.

  Bei späteren Untersuchungen der Quarantäne kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

  Wenn sich eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer späteren Untersuchung als virenfrei erweist, ändert sich ihr Status nur dann *OK*, wenn die Untersuchung der Datei mindestens drei Tage, nachdem sie unter Quarantäne gestellt wurde, stattfindet.
- **Beenden** – Ausführung des Programms abbrechen.
- **Erlauben** - Das Ausführen des Programms erlauben.
- **Zu Ausnahmen hinzufügen** – Dem Programm wird immer erlaubt, solche Aktionen auszuführen.

IN QUARANTÄNE BEFINDLICHE DATEI IST NICHT INFIZIERT

Kaspersky Internet Security untersucht die in Quarantäne befindlichen Dateien automatisch nach jedem Datenbankupdate. Stellt das Programm durch eine Untersuchung einer in Quarantäne befindlichen Datei eindeutig fest, dass diese nicht infiziert ist, erscheint eine entsprechende Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Empfehlung zur Wiederherstellung der in Quarantäne befindlichen Datei;
- Name der Datei, einschließlich des Pfades zum Ordner, in dem sich die Datei bis zu ihrer Verschiebung in die Quarantäne befand.

Ihnen wird angeboten, eine der folgenden Aktionen zu wählen:

- **Wiederherstellen** – Wiederherstellen der Datei durch Entfernen aus der Quarantäne und Ablegen in dem Ordner, in dem sie sich bis zum Verschieben in die Quarantäne befand.

- **Abbrechen** – das Objekt wird in der Quarantäne belassen.

EINE NEUE PRODUKTVERSION IST ERSCHIENEN

Wenn eine neue Version von Kaspersky Internet Security erschienen ist und zum Download auf den Kaspersky-Lab-Servern bereitsteht, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Dieser Link führt zum Fenster mit detaillierten Informationen über die erschienene Programmversion.
- Größe der Installationsdatei

Ihnen wird angeboten, eine der folgenden Aktionen zu wählen:

- **Ja, herunterladen** – Distribution der neuen Programmversion in den festgelegten Ordner herunterladen.
- **Nein** – Download der Distribution verwerfen.

Damit die Meldung über die neue Programmversion nicht mehr angezeigt wird, aktivieren Sie das Kontrollkästchen **Mich nicht über dieses Update informieren**.

EIN TECHNISCHES UPDATE IST ERSCHIENEN

Wenn ein technisches Update für Kaspersky Internet Security erschienen ist und zum Download auf den Kaspersky-Lab-Servern bereitsteht, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Versionsnummer des Programms, das auf dem Computer installiert ist.
- Versionsnummer des Programms nach dem angebotenen technischen Update
- Link zu einem Fenster mit ausführlichen Informationen zum technischen Update
- Größe der Updatedatei

Ihnen wird angeboten, eine der folgenden Aktionen zu wählen:

- **Ja, herunterladen** – Updatedatei in den festgelegten Ordner herunterladen.
- **Nein** – Download des Updates verwerfen. Diese Variante ist verfügbar, wenn das Kontrollkästchen **Mich nicht über dieses Update informieren** aktiviert ist (s. unten).
- **Nein, später erinnern** – Download des Updates jetzt verwerfen und später an das Update erinnern. Diese Variante ist verfügbar, wenn das Kontrollkästchen **Mich nicht über dieses Update informieren** deaktiviert ist (s. unten).

Aktivieren Sie das Kontrollkästchen **Mich nicht über dieses Update informieren**, damit die Meldung über dieses Update nicht mehr angezeigt wird.

EIN TECHNISCHES UPDATE WURDE HERUNTERGELADEN

Nachdem der Download eines technischen Updates für Kaspersky Internet Security abgeschlossen wurde, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Versionsnummer des Programms nach dem technischen Update

- Link zur Updatedatei

Ihnen wird angeboten, eine der folgenden Aktionen zu wählen:

- **Ja, installieren** – Update installieren.

  Nach der Installation des Updates kann ein Neustart des Betriebssystems erforderlich sein.

- **Installation aufschieben** – Installation verwerfen, um sie später auszuführen.

DAS HERUNTERGELADENE TECHNISCHE UPDATE WURDE NICHT INSTALLIERT

Wenn auf Ihrem Computer ein technisches Update für Kaspersky Internet Security vorhanden ist, das früher heruntergeladen wurde, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Versionsnummer des Programms nach dem technischen Update
- Link zur Updatedatei

Ihnen wird angeboten, eine der folgenden Aktionen zu wählen:

- **Ja, installieren** – Update installieren.

  Nach der Installation des Updates kann ein Neustart des Betriebssystems erforderlich sein.

- **Installation aufschieben** – Installation verwerfen, um sie später auszuführen.

Aktivieren Sie das Kontrollkästchen **Bis zum Erscheinen einer neuen Version nicht mehr fragen**, damit die Meldung über dieses Update nicht mehr angezeigt wird.

LIZENZ ABGELAUFEN

Nach Ablauf der Gültigkeitsdauer der Testlizenz zeigt Kaspersky Internet Security auf dem Bildschirm eine Meldung an.

Die Meldung enthält folgende Informationen:

- Dauer des Testzeitraums;
- Informationen über die Ergebnisse der Programmausführung (kann einen Link zum Anzeigen ausführlicherer Daten beinhalten).

Ihnen wird angeboten, eine der folgenden Aktionen zu wählen:

- **Ja, kaufen** – bei Auswahl dieser Option öffnet sich der Browser und lädt die Seite des Webshops, wo Sie eine kommerzielle Lizenz für die Nutzung des Programms erwerben können.
- **Abbrechen** – Verzicht auf die Nutzung des Programms. Bei Auswahl dieser Option stellt das Programm alle seine Hauptfunktionen ein (Virensuche, Echtzeitschutz-Funktionen usw.).

MELDUNGEN IM INTERAKTIVEN SCHUTZMODUS

Dieser Abschnitt enthält alle Meldungen, die bei der Arbeit des Programms im interaktiven Schutzmodus erscheinen können (s. Abschnitt "Schutzmodus auswählen" auf S. 83). Wenn solche Meldungen nicht auf dem Bildschirm angezeigt werden sollen, schalten Sie zum automatischen Schutzmodus um. In diesem Fall erscheinen nur die Meldungen, die in einem beliebigen Schutzmodus (s. Abschnitt "Meldungen in allen Schutzmodi" auf S. 213) zur Anzeige vorgesehen sind.

IN DIESEM ABSCHNITT

Netzwerkaktivität eines Programms wurde erkannt 220

Verdächtiges Objekt wurde gefunden 221

Eine Schwachstelle wurde gefunden 222

Anfrage auf Erlaubnis für Programmaktionen 223

Gefährliche Aktivität im System wurde erkannt 223

Rollback von Änderungen, die von einem gefährlichen Programm ausgeführt wurden. 224

Ein schädliches Programm wurde gefunden 224

Ein verdächtiges Programm oder ein legales Programm, das von Angreifern verwendet werden kann, wurde gefunden 225

Ein verdächtiger / schädlicher Link wurde gefunden 226

Gefährliches Objekt wurde im Datenstrom gefunden 226

Ein versuchter Zugriff auf eine Phishing-Seite wurde erkannt 227

Versuch zum Zugriff auf die Systemregistrierung wurde erkannt 227

Desinfektion des Objekts ist nicht möglich 227

Versteckter Prozess wurde gefunden 228

Geo-Filter hat den Zugriff auf eine Webseite blockiert 229

Web-Filter hat den Download einer Webseite blockiert 229

Web-Filter hat den Download einer Webseite angehalten 230

Es wird empfohlen, in den Sicheren Browsermodus zu wechseln 230

Es wird empfohlen, den Sicheren Browsermodus zu verlassen 230

NETZWERKAKTIVITÄT EINES PROGRAMMS WURDE ERKANNT

Wenn die Netzwerkaktivität eines Programms erkannt wird, erscheint auf dem Bildschirm eine Meldung (standardmäßig für Programme der Gruppen **Schwach beschränkt** oder **Stark beschränkt**).

Es wird eine Meldung angezeigt, wenn Kaspersky Internet Security im interaktiven Modus (s. Abschnitt "Schutzmodus auswählen" auf S. 83), arbeitet und für das Programm, dessen Netzwerkaktivität erkannt wurde, keine Paketregel (s. S. 134) erstellt wurde.

Die Meldung enthält folgende Informationen:

- Name des Programms und kurze Charakteristik der von ihm initiierten Verbindung.
- Informationen zur Verbindung (Verbindungstyp, lokaler Port und Remoteport, Adresse, mit der die Verbindung erfolgt).
- Startfolge eines Programms.

Ihnen wird angeboten, eine der folgenden Aktionen zu wählen:

- **Jetzt erlauben**.
- **Jetzt verbieten**.
- **Regel erstellen**. Bei Auswahl dieser Variante öffnet sich das Fenster **Firewall**, in dem Sie eine Regel erstellen können, mit der die Netzwerkaktivität des Programms reguliert wird (s. Abschnitt "Programmregeln ändern" auf S. 135).

Sie können die Netzwerkaktivität eines Programms einmalig oder für einen längeren Zeitraum verbieten oder erlauben. Führen Sie hierzu eine der folgenden Aktionen aus:

- Um die Netzwerkaktivität eines Programms einmalig zu erlauben oder zu verbieten, wählen Sie bitte **Jetzt erlauben** oder **Jetzt verbieten**.
- Um die ausgewählte Aktion für die gesamte Sitzung des Programms, bei dem eine Netzwerkaktivität festgestellt wurde, zu speichern, wählen Sie **Jetzt erlauben** oder **Jetzt verbieten** aus und aktivieren Sie das Kontrollkästchen **Speichern für diese Programmsitzung**.

  Wird im Fenster das Kontrollkästchen **Speichern für immer** angezeigt, dann aktivieren Sie dieses bitte und betätigen Sie danach den Link **für immer**, um die Bezeichnung in **Speichern für diese Programmsitzung** zu ändern.
- Um die für das Programm ausgewählte Aktion für immer zu speichern, wählen Sie bitte die Aktion **Jetzt erlauben** oder **Jetzt verbieten** und aktivieren Sie das Kontrollkästchen **Speichern für immer**.

  Wird im Fenster das Kontrollkästchen **Speichern für diese Programmsitzung** angezeigt, dann aktivieren Sie dieses bitte und betätigen Sie danach den Link **für die Programmsitzung** zum Ändern der Bezeichnung in **Speichern für immer**.

VERDÄCHTIGES OBJEKT WURDE GEFUNDEN

Wenn von Datei-Anti-Virus, Mail-Anti-Virus oder von einer Untersuchungsaufgabe ein schädliches Objekt gefunden wird, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Art der Bedrohung und Name des schädlichen Objekts gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen eines schädlichen Objekts befindet sich das Symbol . Durch Klick auf das Symbol wird ein Fenster mit Informationen über das Objekt geöffnet. Aus diesem Fenster gelangen Sie über den Link www.securelist.com zur Webseite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen über die Bedrohung erhalten können, die dieses Objekt darstellt.
- Dateiname und Pfad eines schädlichen Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Desinfizieren** – Es wird versucht, das schädliche Objekt zu desinfizieren. Diese Option wird vorgeschlagen, wenn es sich um eine bekannte Bedrohung behandelt, die das Programm zu desinfizieren versuchen kann.

  Vor der Desinfektion wird eine Sicherungskopie des Objekts angelegt, um bei Bedarf das Objekt wiederherstellen oder dessen Infektionsbild konkretisieren zu können.

- **Quarantäne** – Objekt in die Quarantäne verschieben, wo es keine Gefahr für Ihren Computer darstellt. Diese Option wird vorgeschlagen, wenn es sich um eine unbekannte Bedrohung behandelt, für die bislang keine Desinfektionsmethoden bekannt sind.

  Bei späteren Untersuchungen der Quarantäne kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

  Wenn sich eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer späteren Untersuchung als virenfrei erweist, ändert sich ihr Status nur dann *OK*, wenn die Untersuchung der Datei mindestens drei Tage, nachdem sie unter Quarantäne gestellt wurde, stattfindet.

- **Löschen** – Das Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt, um das Objekt bei Bedarf beispielsweise wiederherstellen oder dessen Infektionsbild konkretisieren zu können.

- **Überspringen / Blockieren** – Der Zugriff auf das Objekt wird gesperrt. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

  Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

Damit die gewählte Aktion auf alle Objekte mit diesem Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

EINE SCHWACHSTELLE WURDE GEFUNDEN

Wenn bei der Ausführung einer Untersuchungsaufgabe eine Schwachstelle gefunden wird, erscheint eine Meldung auf dem Bildschirm.

Sie enthält folgende Informationen:

- Beschreibung der Schwachstelle

- Name der Schwachstelle gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen befindet sich das Symbol . Durch Klick auf das Symbol wird ein Fenster mit Informationen über die Schwachstelle geöffnet. Aus diesem Fenster gelangen Sie über den Link www.securelist.com zur Webseite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen über die Schwachstelle erhalten können.

- Dateiname und Pfad des anfälligen Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Ja, korrigieren** – Schwachstelle beheben.

- **Überspringen** – Keine Aktionen mit dem anfälligen Objekt ausführen.

ANFRAGE AUF ERLAUBNIS FÜR PROGRAMMAKTIONEN

Wenn ein Programm versucht, eine Aktion auszuführen, über deren Sicherheit oder Notwendigkeit Kaspersky Internet Security keine Informationen vorliegen, so erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Name und Symbol des Programms Durch Klick auf das Symbol wird ein Fenster mit Informationen über das Programm geöffnet.
- Beschreibung der Programmaktionen
- Ort der Programmdatei
- Startfolge des Programms

Sie können die Ausführung des Programms erlauben oder verbieten. Wählen Sie dazu eine der folgenden Aktionen:

- **Vertrauenswürdig machen** – Programm in die vertrauenswürdige Gruppe aufnehmen, damit seine Ausführung immer erlaubt wird.
- **Jetzt erlauben** – Ausführung des Programms einmal erlauben.
- **Jetzt verbieten** – Ausführung des Programms einmal verbieten.
- **Programm beenden und als nicht vertrauenswürdig einstufen** – Programm in die nicht vertrauenswürdige Gruppe aufnehmen, damit seine Ausführung immer verboten wird.

GEFÄHRLICHE AKTIVITÄT IM SYSTEM WURDE ERKANNT

Wenn der Proaktive Schutz die gefährliche Aktivität einer bestimmten Anwendung im System erkennt, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Art der Bedrohung und Name des schädlichen Objekts gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen eines schädlichen Objekts befindet sich das Symbol . Durch Klick auf das Symbol wird ein Fenster mit Informationen über das Objekt geöffnet. Aus diesem Fenster gelangen Sie über den Link www.securelist.com zur Webseite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen über die Bedrohung erhalten können, die dieses Objekt darstellt.
- Prozess-ID, Name und Pfad der Programmdatei.

Folgende Aktionen stehen zur Auswahl:

- **Quarantäne** – Programm beenden und Programmdatei in die Quarantäne verschieben, wo sie keine Gefahr für Ihren Computer darstellt.

  Bei späteren Untersuchungen der Quarantäne kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

  Wenn sich eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer späteren Untersuchung als virenfrei erweist, ändert sich ihr Status nur dann *OK*, wenn die Untersuchung der Datei mindestens drei Tage, nachdem sie unter Quarantäne gestellt wurde, stattfindet.
- **Beenden** – Ausführung des Programms abbrechen.

- **Erlauben** - Das Ausführen des Programms erlauben.
- **Zu Ausnahmen hinzufügen** – Dem Programm wird immer erlaubt, solche Aktionen auszuführen.

Damit die ausgewählte Aktion auf alle Objekte mit diesem Status angewendet wird, die während der laufenden Sitzung des Proaktiven Schutzes gefunden werden, aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms.

Wenn Sie überzeugt sind, dass das gefundene Programm ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass Kaspersky Internet Security erneut anspricht, wenn er das Programm findet.

ROLLBACK VON ÄNDERUNGEN, DIE VON EINEM GEFÄHRLICHEN PROGRAMM AUSGEFÜHRT WURDEN.

Nachdem die Ausführung eines potentiell gefährlichen Programms abgeschlossen wurde, wird empfohlen, die Veränderungen im System rückgänig zu machen (zu verwerfen). In diesem Fall erscheint auf dem Bildschirm eine Meldung mit einer Anfrage für ein Rollback der Veränderungen.

Die Meldung enthält folgende Informationen:

- Anfrage auf ein Rollback von Veränderungen, die das potentiell gefährliche Programm ausgeführt hat.
- Typ und Name des Programms

  Neben dem Namen des Programms befindet sich das Symbol . Durch Klick auf das Symbol wird ein Fenster mit Informationen über das Programm geöffnet.
- Prozess-ID, Name und Pfad der Programmdatei.

Folgende Aktionen stehen zur Auswahl:

- **Ja, rückgängig machen** – Es wird versucht, die von diesem Programm ausgeführten Veränderungen rückgängig zu machen.
- **Überspringen** – Veränderungen nicht rückgängig machen.

EIN SCHÄDLICHES PROGRAMM WURDE GEFUNDEN

Wenn der Aktivitätsmonitor ein Programm erkennt, dessen Verhalten genau mit den Aktionen von Schadprogrammen übereinstimmt, so erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Typ und Name des schädlichen Programms

  Neben dem Namen des Programms befindet sich das Symbol . Durch Klick auf das Symbol wird ein Fenster mit Informationen über das Programm geöffnet.
- Prozess-ID, Name und Pfad der Programmdatei.
- Dieser Link führt zum Fenster mit einem Ereignisverlauf für das Programm.

Folgende Aktionen stehen zur Auswahl:

- **Quarantäne** – Programm beenden und Programmdatei in die Quarantäne verschieben, wo sie keine Gefahr für Ihren Computer darstellt.

Bei späteren Untersuchungen der Quarantäne kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

Wenn sich eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer späteren Untersuchung als virenfrei erweist, ändert sich ihr Status nur dann *OK*, wenn die Untersuchung der Datei mindestens drei Tage, nachdem sie unter Quarantäne gestellt wurde, stattfindet.

- **Beenden** – Ausführung des Programms abbrechen.
- **Erlauben** - Das Ausführen des Programms erlauben.
- **Zu Ausnahmen hinzufügen** – Dem Programm wird immer erlaubt, solche Aktionen auszuführen.

EIN VERDÄCHTIGES PROGRAMM ODER EIN LEGALES PROGRAMM, DAS VON ANGREIFERN VERWENDET WERDEN KANN, WURDE GEFUNDEN

Wenn von Datei-Anti-Virus, Mail-Anti-Virus oder von einer Untersuchungsaufgabe ein verdächtiges Programm oder ein legales Programm gefunden wird, das von Angreifern verwendet werden kann, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Art der Bedrohung und Name des Objekts gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen eines Objekts befindet sich das Symbol . Durch Klick auf das Symbol wird ein Fenster mit Informationen über das Objekt geöffnet. Aus diesem Fenster gelangen Sie über den Link www.securelist.com zur Seite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen erhalten können.
- Dateiname und Pfad des Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Quarantäne** – Objekt in die Quarantäne verschieben, wo es keine Gefahr für Ihren Computer darstellt. Diese Option wird vorgeschlagen, wenn es sich um eine unbekannte Bedrohung behandelt, für die bislang keine Desinfektionsmethoden bekannt sind.

  Bei späteren Untersuchungen der Quarantäne kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

  Wenn sich eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer späteren Untersuchung als virenfrei erweist, ändert sich ihr Status nur dann *OK*, wenn die Untersuchung der Datei mindestens drei Tage, nachdem sie unter Quarantäne gestellt wurde, stattfindet.
- **Löschen** – Das Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt, um das Objekt bei Bedarf beispielsweise wiederherstellen oder dessen Infektionsbild konkretisieren zu können.
- **Archiv löschen** - kennwortgeschütztes Archiv löschen.
- **Überspringen / Blockieren** – Der Zugriff auf das Objekt wird gesperrt. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

  Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).
- **Zu Ausnahmen hinzufügen** - für diesen Bedrohungstyp eine Ausnahmeregel erstellen.

Damit die gewählte Aktion auf alle Objekte mit diesem Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

Wenn Sie überzeugt sind, dass das gefundene Objekt ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass das Programm bei der Arbeit mit diesem Objekt erneut anspricht.

EIN VERDÄCHTIGER / SCHÄDLICHER LINK WURDE GEFUNDEN

Wenn Kaspersky Internet Security erkennt, dass versucht wird, eine Webseite mit schädlichem oder verdächtigem Inhalt zu öffnen, erscheint auf dem Bildschirm eine spezielle Meldung.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Name des Programms (Browsers), mit dem das Laden der Webseite ausgeführt wird.
- Adresse der Website oder Webseite mit schädlichem oder verdächtigem Inhalt.

Folgende Aktionen stehen zur Auswahl:

- **Erlauben** – Download der Webseite fortsetzen.
- **Verbieten** – Download der Webseite blockieren.

Damit die gewählte Aktion auf alle Webseiten mit diesem Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente gefunden werden, aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms.

GEFÄHRLICHES OBJEKT WURDE IM DATENSTROM GEFUNDEN

Wenn Web-Anti-Virus im Datenstrom ein gefährliches Objekt findet, erscheint eine spezielle Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung oder der Aktionen, die ein Programm ausführen kann.
- Name des Programms, das eine Aktion ausführt.
- Art der Bedrohung und Name des schädlichen Objekts gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen eines schädlichen Objekts befindet sich das Symbol . Durch Klick auf das Symbol wird ein Fenster mit Informationen über das Objekt geöffnet. Aus diesem Fenster gelangen Sie über den Link www.securelist.com zur Webseite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen über die Bedrohung erhalten können, die dieses Objekt darstellt.
- Ort des Objekts (Webadresse).

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Erlauben**- Download des Objekts fortsetzen.
- **Verbieten** – Download des Objekts von der Webressource blockieren.

Damit die gewählte Aktion auf alle Objekte mit diesem Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

EIN VERSUCHTER ZUGRIFF AUF EINE PHISHING-SEITE WURDE ERKANNT

Wenn Kaspersky Internet Security erkennt, dass versucht wird, auf eine Webseite zuzugreifen, die als Phishing-Seite bekannt ist oder des Phishings verdächtig ist, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Adresse der Webseite im Internet

Ihnen wird angeboten, eine der folgenden Aktionen zu wählen:

- **Erlauben** – Download der Webseite fortsetzen.
- **Verbieten** – Download der Webseite blockieren.

Damit die gewählte Aktion auf alle Webseiten mit diesem Status angewendet wird, die während der laufenden Sitzung von Kaspersky Internet Security gefunden werden, aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms.

VERSUCH ZUM ZUGRIFF AUF DIE SYSTEMREGISTRIERUNG WURDE ERKANNT

Wenn der Proaktive Schutz erkennt, dass versucht wird, auf Schlüssel der Systemregistrierung zuzugreifen, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Registrierungsschlüssel, auf den der Zugriffsversuch erfolgte.
- Dateiname und Pfad des Prozesses, der versucht hat auf Registrierungsschlüssel zuzugreifen.

Ihnen wird angeboten, eine der folgenden Aktionen zu wählen:

- **Erlauben** - Das Ausführen der gefährlichen Aktion einmal erlauben.
- **Verbieten** - Das Ausführen der gefährlichen Aktion einmal verbieten.

Damit die von Ihnen ausgewählte Aktion jedes Mal automatisch ausgeführt wird, wenn diese Aktivität auf Ihrem Computer initiiert wird, aktivieren Sie das Kontrollkästchen **Regel erstellen**.

Wenn Sie überzeugt sind, dass jede Aktivität der Anwendung, die den Zugriff auf die Systemregistrierungsschlüssel initiierte, ungefährlich ist, fügen Sie diese Anwendung der Liste der vertrauenswürdigen Anwendungen hinzu.

DESINFEKTION DES OBJEKTS IST NICHT MÖGLICH

Es kann vorkommen, dass sich ein schädliches Objekt nicht desinfizieren lässt, weil die Datei so stark beschädigt ist, dass der schädliche Code nicht daraus gelöscht und sie vollständig wiederhergestellt werden kann. Außerdem ist die Desinfektionsprozedur nicht einige Arten von schädlichen Objekten wie z.B. Trojaner-Programme nicht anwendbar. In diesem Fall erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Art der Bedrohung und Name des schädlichen Objekts gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen eines schädlichen Objekts befindet sich das Symbol. Durch Klick auf das Symbol wird ein Fenster mit Informationen über das Objekt geöffnet. Aus diesem Fenster gelangen Sie über den Link www.securelist.com zur Webseite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen über die Bedrohung erhalten können, die dieses Objekt darstellt.
- Dateiname und Pfad eines schädlichen Objekts.

Ihnen wird angeboten, eine der folgenden Aktionen für das Objekt auszuwählen:

- **Löschen** – Das Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt, um das Objekt bei Bedarf beispielsweise wiederherstellen oder dessen Infektionsbild konkretisieren zu können.
- **Überspringen / Blockieren** – Der Zugriff auf das Objekt wird gesperrt. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

  Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

Damit die gewählte Aktion auf alle Objekte mit diesem Status angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms, sowie die Ausführungszeit einer Untersuchungsaufgabe ab dem Start bis zum Abschluss.

VERSTECKTER PROZESS WURDE GEFUNDEN

Wenn der Proaktive Schutz einen versteckten Prozess im System findet, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Art und Name der Bedrohung gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen befindet sich das Symbol. Durch Klick auf das Symbol wird ein Fenster mit Informationen über die Bedrohung geöffnet. Aus diesem Fenster gelangen Sie über den Link www.securelist.com zur Seite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen über die Bedrohung erhalten können.
- Name und Pfad der Prozessdatei

Ihnen wird angeboten, eine der folgenden Aktionen zu wählen:

- **Quarantäne** – Prozess beenden und Prozessdatei in die Quarantäne verschieben, wo sie keine Gefahr für Ihren Computer darstellt.

  Bei späteren Untersuchungen der Quarantäne kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

  > Wenn sich eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer späteren Untersuchung als virenfrei erweist, ändert sich ihr Status nur dann *OK*, wenn die Untersuchung der Datei mindestens drei Tage, nachdem sie unter Quarantäne gestellt wurde, stattfindet.
- **Beenden** – Prozess abbrechen.

- **Erlauben** - Das Ausführen des Prozesses erlauben.

Damit die gewählte Aktion auf alle versteckten Prozesse mit diesem Status angewendet wird, die während der laufenden Sitzung des Proaktiven Schutzes gefunden werden, aktivieren Sie das Kontrollkästchen **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente ab dem Zeitpunkt ihres Starts bis zum Moment des Abschaltens oder Neustarts des Programms.

Wenn Sie überzeugt sind, dass der gefundene Prozess ungefährlich ist, können Sie ihn der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass Kaspersky Internet Security erneut anspricht, wenn er den Prozess findet.

GEO-FILTER HAT DEN ZUGRIFF AUF EINE WEBSEITE BLOCKIERT

Web-Anti-Virus kann den Zugriff auf eine Webseite auf Basis ihrer Zugehörigkeit zu einer regionalen Domain blockieren. Eine Domain gilt in folgenden Fällen als verboten:

- Zugriff auf die Domain wurde vom Benutzer bei der Konfiguration von Web-Anti-Virus verboten.
- Ein vorhergehender Zugriff auf eine Webseite aus dieser Region wurde vom Benutzer verboten.

Wenn der Geo-Filter (Modul von Web-Anti-Virus) erkennt, dass versucht wird, eine Webseite zu öffnen, die einer verbotenen Region angehört, erscheint eine Meldung im Browserfenster.

Die Meldung enthält folgende Informationen:

- Beschreibung des Grunds, aus dem der Zugriff auf die Webseite blockiert wurde.
- Name der Region, zu der die Webseite gehört.
- Domain und Beschreibung des Kontaminationsgrads der Webseiten in dieser Domain
- Adresse der Webseite

Folgende Aktionen stehen zur Auswahl:

- **Zur vorherigen Seite zurückkehren** – Vorherige Webseite öffnen.
- **Webressource öffnen** – Webseite, die zu einer verbotenen Domain gehört, laden.
- **Einstellungen für Geo-Filter öffnen** – Konfigurationsfenster für Web-Anti-Virus auf der Registerkarte **Geo-Filter** öffnen.

WEB-FILTER HAT DEN DOWNLOAD EINER WEBSEITE BLOCKIERT

Wenn der Web-Filter (Modul von Web-Anti-Virus) erkennt, dass versucht wird, eine gefährliche Webseite zu öffnen, erscheint eine Meldung im Browserfenster.

Die Meldung enthält folgende Informationen:

- Beschreibung des Grunds, aus dem der Zugriff auf die Webseite blockiert wurde.
- Adresse der Webseite

Folgende Aktionen stehen zur Auswahl:

- **Zur vorherigen Seite zurückkehren** – Vorherige Webseite öffnen.
- **In jedem Fall öffnen** – Webseite laden, obwohl sie riskant ist.

WEB-FILTER HAT DEN DOWNLOAD EINER WEBSEITE ANGEHALTEN

Wenn der Web-Filter (Modul von Web-Anti-Virus) erkennt, dass versucht wird, eine Webseite zu öffnen, über die keine zuverlässigen Sicherheitsdaten vorliegen, so erscheint eine Meldung im Browserfenster.

Die Meldung enthält folgende Informationen:

- Beschreibung des Grunds, aus dem der Zugriff auf die Webseite angehalten wurde.
- Adresse der Webseite

Folgende Aktionen stehen zur Auswahl:

- **Ja, Webressource öffnen** – Webseite laden.
- **Öffnen und zu vertrauenswürdigen Adressen hinzufügen** – Webseite laden und ihre Adresse zur vertrauenswürdigen Liste hinzufügen, damit der Web-Filter das Laden dieser Webseite künftig nicht mehr anhält.
- **Im Sicheren Browser öffnen** – Webseite im Sicheren Browser laden (nur für die Browser Microsoft Internet Explorer, Mozilla Firefox und Google Chrome). Wenn schädliche Objekte, die sich auf zu ladenden Seiten befinden, imSicheren Browser geladen werden, stellen sie keine Gefahr für die Computersicherheit dar.
- **Nein, zur vorherigen Seite zurückkehren** – Webseite nicht laden und vorherige Seite öffnen.

ES WIRD EMPFOHLEN, IN DEN SICHEREN BROWSERMODUS ZU WECHSELN

Beim Online-Banking benötigt der Benutzer einen besonderen Schutz, da ein Verlust sensibler Daten in diesem Fall zu finanziellen Nachteilen führen kann. Aus diesem Grund empfiehlt Kaspersky Lab für das Online-Banking den Einsatz des Sicheren Browsers, der Ihren persönlichen Daten erhöhte Sicherheit bietet.

Wenn versucht wird, eine Webseite für Online-Banking zu öffnen, zeigt Web-Anti-Virus im Browserfenster eine Meldung an.

Die Meldung enthält folgende Informationen:

- Empfehlung, in den Sicheren Modus zu wechseln.
- Adresse der Ressource für Online-Banking.

Ihnen wird angeboten, eine der folgenden Aktionen zu wählen:

- **Im Modus "Sicherer Browser" öffnen** – Webseite unter Verwendung des Sicheren Browsers öffnen (nur für die Browser Microsoft Internet Explorer, Mozilla Firefox und Google Chrome).
- **Webseite öffnen** – Webseite im normalen Modus öffnen.
- **Zur vorherigen Seite zurückkehren** – Vorherige Webseite im normalen Modus öffnen.

ES WIRD EMPFOHLEN, DEN SICHEREN BROWSERMODUS ZU VERLASSEN

Wenn Sie im Sicheren Browsermodus mit einer Webseite für Online-Banking arbeiten und auf eine andere Webseite wechseln, die nichts mit Online-Banking zu tun hat, wird empfohlen, den Sicheren Browsermodus zu verlassen. Wenn Sie im Sicheren Browser mit einer gewöhnlichen Webseite weiterarbeiten, kann dies den Schutz Ihrer persönlichen Daten beeinträchtigen.

Wenn im Sicheren Browsermodus versucht wird, von einer Webseite für Online-Banking auf eine andere Webseite zu wechseln, zeigt Web-Anti-Virus im Browserfenster eine Meldung an.

Die Meldung enthält folgende Informationen:

- Empfehlung, den Sicheren Browsermodus zu verlassen.
- Adresse der Webseite, auf die Sie von der Online-Banking-Seite aus wechseln möchten.

Ihnen wird angeboten, eine der folgenden Aktionen zu wählen:

- **Seite im normalen Modus öffnen** – Sicheren Browsermodus verlassen und Webseite, die nichts mit Online-Banking zu tun hat, im normalen Modus öffnen.
- **Sicheren Browsermodus fortsetzen** – Im Sicheren Browsermodus bleiben und Webseite, die nichts mit Online-Banking zu tun hat, öffnen.
- **Zur vorherigen Seite zurückkehren** – Vorherige Webseite im Sicheren Browsermodus öffnen.

BEDIENUNG DES PROGRAMMS ÜBER DIE BEFEHLSZEILE

Sie können Kaspersky Internet Security mit Hilfe der Befehlszeile steuern. Dabei ist die Möglichkeit zum Ausführen der folgenden Operationen vorgesehen:

- Programm aktivieren
- Programm starten und beenden
- Programmkomponenten starten und beenden.
- Aufgaben starten und beenden
- Erhalt von Informationen über den aktuellen Status von Komponenten und Aufgaben und ihrer Statistik.
- Ausführung von Untersuchungsaufgaben starten und beenden.
- Untersuchung von ausgewählten Objekten.
- Update der Datenbanken und Programm-Module, Rollback von Updates.
- Export und Import von Schutzparametern.
- Aufruf der Hilfe über die Syntax der Befehlszeile insgesamt und für einzelne Befehle.

Syntax der Befehlszeile:

```
avp.com <Befehl> [Parameter]
```

Der Zugriff auf das Programm über die Befehlszeile muss aus dem Installationsordner des Produkts oder unter Angabe des vollständigen Pfads von avp.com erfolgen.

Die Liste der Befehle, die für die Steuerung des Programms und seiner Komponenten verwendet werden, finden Sie in der nachstehenden Tabelle.

START	Komponente oder Aufgabe starten
STOP	Beenden der Arbeit einer Komponente oder Aufgabe (die Ausführung des Befehls ist nur möglich, wenn das Kennwort eingegeben wird, das auf dem Interface von Kaspersky Internet Security festgelegt wurde)
STATUS	Bildschirmanzeige des aktuellen Status einer Komponente oder Aufgabe

STATISTICS	Bildschirmanzeige der Statistik über die Arbeit einer Komponente oder Aufgabe
HELP	Anzeige der Befehlsliste sowie von Informationen über die Befehlssyntax auf dem Bildschirm
SCAN	Untersuchung von Objekten auf das Vorhandensein von Viren
UPDATE	Programm-Update starten
ROLLBACK	Rückgängigmachen des zuletzt durchgeführten Updates von Kaspersky Internet Security (die Ausführung des Befehls ist nur möglich, wenn das Kennwort eingegeben wird, das über die Programmoberfläche festgelegt wurde)
EXIT	Beenden der Arbeit mit dem Programm (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)
IMPORT	Importieren von Schutzeinstellungen für Kaspersky Internet Security (die Ausführung des Befehls ist nur möglich, wenn über die Programmoberfläche festgelegte Kennwort angegeben wird)
EXPORT	Schutzparameter des Programms exportieren

Jedem Befehl entspricht eine eigene Auswahl von Parametern, die für eine konkrete Komponente des Programms spezifisch sind.

IN DIESEM ABSCHNITT

Programm aktivieren 232

Programm starten 233

Programm beenden 233

Steuerung von Komponenten und Aufgaben des Programms 233

Virensuche 235

Programm-Update 237

Rollback zum vorherigen Update 238

Schutzparameter exportieren 238

Schutzparameter importieren 239

Protokolldatei anlegen 239

Hilfe anzeigen 240

Rückgabecodes der Befehlszeile 240

PROGRAMM AKTIVIEREN

Kaspersky Internet Security kann mit Hilfe einer Schlüseldatei aktiviert werden.

Befehlssyntax:

```
avp.com ADDKEY <Dateiname>
```

Eine Beschreibung der Parameter für die Befehlsausführung ist in der nachstehenden Tabelle zu finden.

<Dateiname>	Name der Lizenzschlüsseldatei für das Programm (Endung .key).

Beispiel:

```
avp.com ADDKEY 1AA111A1.key
```

PROGRAMM STARTEN

Befehlssyntax:

```
avp.com
```

PROGRAMM BEENDEN

Befehlssyntax:

```
avp.com EXIT /password=<Kennwort>
```

Folgende Tabelle beschreibt die Parameter.

<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.

Beachten Sie, dass dieser Befehl nicht ausgeführt wird, wenn das Kennwort nicht eingegeben wird.

STEUERUNG VON KOMPONENTEN UND AUFGABEN DES PROGRAMMS

Befehlssyntax:

```
avp.com <Befehl> <Profil|Aufgabenname> [/R[A]:<Berichtsdatei>]
avp.com STOP <Profil|Aufgabenname>  /password=<Kennwort> [/R[A]:<Berichtsdatei>]
```

Befehle und Parameter werden in folgender Tabelle beschrieben.

<Befehl>	Die Steuerung der Komponenten und Aufgaben von Kaspersky Internet Security wird mit Hilfe der folgenden Befehle ausgeführt: START – Start einer Schutzkomponente oder einer Aufgabe. STOP – Beenden einer Schutzkomponente oder einer Aufgabe. STATUS – Aktuellen Status einer Komponente oder Aufgabe auf dem Bildschirm anzeigen. STATISTICS – Die Statistik über die Arbeit einer Schutzkomponente oder einer Aufgabe auf dem Bildschirm anzeigen. Beachten Sie, dass der Befehl STOP nur ausgeführt wird, wenn das Kennwort eingegeben wird.
<Profil|Aufgabenname>	Als Wert für den Parameter **<Profil>** sind möglich: eine beliebige Schutzkomponente von Kaspersky Internet Security, Module, die zu den Komponenten gehören, erstellte Untersuchungs- oder Updateaufgaben (die vom Programm standardmäßig verwendeten Werte werden in folgender Tabelle genannt). Als Wert für den Parameter **<Aufgabenname>** kann der Name einer beliebigen vom Benutzer erstellten Untersuchungs- oder Updateaufgabe angegeben werden.

<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.
/R[A]:<Berichtsdatei>	**/R:<Berichtsdatei>** – nur wichtige Ereignisse im Bericht protokollieren. **/RA:<Berichtsdatei>** - alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

Für den Parameter **<Profil>** wird einer der Werte aus folgender Tabelle angegeben.

RTP	Alle Schutzkomponenten. Der Befehl **avp.com START RTP** startet alle Schutzkomponenten, wenn der Schutz vollständig deaktiviert war. Wenn eine Komponente mit dem Befehl **STOP** aus der Befehlszeile beendet wurde, wird sie durch den Befehl **avp.com START RTP** nicht gestartet. Um die Komponente zu starten, ist der Befehl **avp.com START <Profil>** erforderlich, wobei als **<Profil>** der Wert der betreffenden Schutzkomponente verwendet wird, beispielsweise **avp.com START FM**.
FW	Firewall.
HIPS	Programmkontrolle aus.
pdm	Proaktiver Schutz.
FM	Datei-Anti-Virus.
EM	Mail-Anti-Virus.
WM	Web-Anti-Virus. Werte für die Subkomponenten von Web-Anti-Virus: **httpscan (HTTP)** – Untersuchung des http-Datenstroms **sc** – Skript-Untersuchung
IM	IM-Anti-Virus.
AB	Anti-Banner
AS	Anti-Spam.
PC	Kindersicherung.
AP	Anti-Phishing.
ids	Schutz vor Netzwerkangriffen.
Updater	Update.
Rollback	Rollback zum vorherigen Update.
Scan_My_Computer	Untersuchung des Computers.
Scan_Objects	Objekte untersuchen.
Scan_Quarantine	Quarantäne untersuchen.

Scan_Startup (STARTUP)	Autostart-Objekte untersuchen.
Scan_Vulnerabilities (SECURITY)	Schwachstellensuche.

Die aus der Befehlszeile gestarteten Komponenten und Aufgaben werden mit den Parametern ausgeführt, die über die Programmoberfläche festgelegt wurden.

Beispiele:

- *Geben Sie folgenden Befehl ein, um Datei-Anti-Virus zu aktivieren:*

```
avp.com START FM
```

- *Geben Sie folgenden Befehl ein, um die Untersuchung des Computers abzubrechen:*

```
avp.com STOP Scan_My_Computer /password=<Kennwort>
```

VIRENSUCHE

Die Befehlszeile zum Starten der Virenuntersuchung eines bestimmten Bereichs und zum Starten der Verarbeitung von schädlichen Objekten besitzt folgendes allgemeines Aussehen:

```
avp.com SCAN [<Untersuchungsobjekt>] [<Aktion>] [<Dateitypen>] [<Ausnahmen>]
[<Konfigurationsdatei>] [<Berichtsparameter>] [<zusätzliche Parameter>]
```

Für die Untersuchung von Objekten können Sie auch die im Programm erstellten Aufgaben verwenden, die aus der Befehlszeile gestartet werden können. Dabei wird die Aufgabe mit den Parametern ausgeführt, die über die Oberfläche von Kaspersky Internet Security festgelegt wurden.

Folgende Tabelle beschreibt die Parameter.

<Untersuchungsobjekt> – Der Parameter gibt eine Liste der Objekte an, die auf das Vorhandensein von schädlichem Code untersucht werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.	
<files>	Liste mit den Pfaden der Dateien und Ordner für die Untersuchung. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Als Trennzeichen für die Elemente der Liste dient das Leerzeichen. Kommentare: • Wenn der Objektname ein Leerzeichen enthält, wird er in Anführungszeichen gesetzt. • Wenn ein konkreter Ordner angegeben wird, werden alle darin enthaltenen Dateien untersucht.
/MEMORY	Objekte des Arbeitsspeichers.
/STARTUP	Autostart-Objekte**.**
/MAIL	Posteingänge.
/REMDRIVES	Alle Wechseldatenträger.
/FIXDRIVES	Alle lokalen Laufwerke.
/NETDRIVES	Alle Netzlaufwerke.
/QUARANTINE	Objekte in Quarantäne.

/ALL	Vollständige Untersuchung des Computers.
/@:<filelist.lst>	Pfad der Datei mit einer Liste der Objekte und Ordner, die untersucht werden sollen. Für die Datei mit der Liste ist die Angabe des absoluten oder relativen Pfads zulässig. Der Pfad wird ohne Anführungszeichen angegeben, selbst wenn er ein Leerzeichen enthält. Die Datei mit der Liste muss das Textformat besitzen. Jedes Untersuchungsobjekt muss in einer separaten Zeile stehen. Es wird empfohlen, in der Datei die absoluten Pfade der Untersuchungsobjekte anzugeben. Bei Angabe eines relativen Pfads wird der Pfad im Bezug auf die ausführbare Programmdatei angegeben, nicht im Bezug auf die Datei mit der Liste der Untersuchungsobjekte.
<Aktion> – Der Parameter bestimmt die Aktionen mit einem schädlichen Objekt, das während der Untersuchung gefunden wird. Wenn der Parameter nicht angegeben wird, wird standardmäßig die Aktion ausgeführt, die dem Wert **/i8** entspricht. Wenn Sie im automatischen Modus arbeiten, wendet Kaspersky Internet Security beim Fund gefährlicher Objekte automatisch die von Kaspersky Lab empfohlene Aktion an. Die Aktion ausgeführt, die dem **<Aktion>** entspricht, wird ignoriert.	
/i0	Keine Aktion ausführen, Informationen im Bericht protokollieren.
/i1	Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – überspringen**.**
/i2	Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; infizierte Objekte aus Containern (zusammengesetzten Objekten) nicht löschen; Container mit ausführbarer Kopfzeile (sfx-Archive) löschen.
/i3	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
/i4	infizierte Objekte löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
/i8	Beim Fund eines infizierten Objekts den Benutzer nach der Aktion fragen.
/i9	Den Benutzer nach der Aktion fragen, wenn die Untersuchung abgeschlossen wird.
<Dateitypen> – Der Parameter bestimmt die Typen der Dateien, die der Virenuntersuchung unterzogen werden. Wenn der Parameter nicht angegeben wird, werden standardmäßig nur infizierbare Dateien nach ihrem Inhalt untersucht.	
/fe	Nur infizierbare Dateien nach Erweiterung untersuchen.
/fi	Nur infizierbare Dateien nach Inhalt untersuchen.
/fa	**Alle Dateien untersuchen**.
<Ausnahmen> – Der Parameter bestimmt die Objekte, die von der Untersuchung ausgeschlossen werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.	
-e:a	Archive nicht untersuchen.
-e:b	Mail-Datenbanken nicht untersuchen.
-e:m	E-Mail-Nachrichten im Format plain text nicht untersuchen.
-e:<filemask>	Objekte nach Maske nicht untersuchen.

-e:<seconds>	Objekte überspringen, deren Untersuchung länger dauert, als der durch den Parameter **<seconds>** angegebene Zeitraum.
-es:<size>	Objekte überspringen, deren Größe (in MB) über dem Wert liegt, der durch den Parameter **<size>** angegeben wird. Der Parameter ist nur auf zusammengesetzte Dateie (z.B. Archive) anwendbar.
<Konfigurationsdatei> – bestimmt den Pfad der Konfigurationsdatei, in der die Parameter für die Arbeit des Programms bei der Untersuchung enthalten sind. Die Konfigurationsdatei ist eine Datei im Textformat, die eine Auswahl von Befehlszeilenparametern für die Antiviren-Untersuchung enthält. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die über die Programmoberfläche festgelegt wurden.	
/C:<Dateiname>	Die Werte der Parameter, die in der Datei **<Dateiname>** angegeben sind, verwenden.
<Berichtsparameter> – Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.	
/R:<Berichtsdatei>	Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren.
/RA:<Berichtsdatei>	Alle wichtigen Ereignisse in der angegebenen Berichtsdatei protokollieren.
<zusätzliche Parameter> – Parameter, der die Verwendung von Technologien zur Virenuntersuchung festlegt.	
/iChecker=<on|off>	Verwendung der Technologie iChecker aktivieren / deaktivieren.
/iSwift=<on|off>	Verwendung der Technologie iSwift aktivieren / deaktivieren.

Beispiele:

- *Untersuchung des Arbeitsspeichers, der Autostart-Objekte, der Mailboxen sowie der Ordner Eigene Dateien, Programme und der Datei test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My
Documents" "C:\Program Files" "C:\Downloads\test.exe"
```

- *Untersuchung der Objekte, deren Liste in der Datei object2scan.txt angegeben ist. Für die Arbeit soll die Konfigurationsdatei scan_settings.txt verwendet werden. Über die Untersuchungsergebnisse soll ein Bericht erstellt werden, in dem alle Ereignisse aufgezeichnet werden:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Beispiel für die Konfigurationsdatei:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

PROGRAMM-UPDATE

Der Befehl für das Update der Programm-Module und Datenbanken von Kaspersky Internet Security besitzt folgende Syntax:

```
avp.com UPDATE [<Updatequelle>] [/R[A]:<Berichtsdatei>] [/C:<Dateiname>]
```

Folgende Tabelle beschreibt die Parameter.

<Updatequelle>	HTTP-, FTP-Server oder Netzwerkordner für den Download von Updates. Als Wert für diesen Parameter kann der vollständige Pfad oder die URL-Adresse der Updatequelle angegeben werden. Wenn der Pfad nicht angegeben wird, wird die Updatequelle aus den Parametern des Diensts für das Programm-Update übernommen.
/R[A]:<Berichtsdatei>	**/R:**<Berichtsdatei> – nur wichtige Ereignisse im Bericht protokollieren.

	/RA:<Berichtsdatei> - alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.
/C:<Dateiname>	Pfad der Konfigurationsdatei, die die Parameter für die Arbeit von Kaspersky Internet Security beim Update enthält. Die Konfigurationsdatei ist eine Textdatei, die eine Auswahl von Befehlszeilenparametern für das Update des Programms enthält. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die über die Programmoberfläche festgelegt wurden.

Beispiele:

- *Update der Programm-Datenbanken, alle Ereignisse im Bericht protokollieren:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Update der Programm-Module von Kaspersky Internet Security, die Parameter der Konfigurationsdatei updateapp.ini verwenden:*

```
avp.com UPDATE /C:updateapp.ini
```

Beispiel für die Konfigurationsdatei:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK ZUM VORHERIGEN UPDATE

Befehlssyntax:

```
avp.com ROLLBACK [/R[A]:<Berichtsdatei>][/password=<Kennwort>]
```

Folgende Tabelle beschreibt die Parameter.

/R[A]:<Berichtsdatei>	**/R:**<Berichtsdatei> – nur wichtige Ereignisse im Bericht protokollieren. **/RA:**<Berichtsdatei> - alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.
<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.

Beachten Sie, dass dieser Befehl nicht ausgeführt wird, wenn das Kennwort nicht eingegeben wird.

Beispiel:

```
avp.com ROLLBACK /RA:rollback.txt /password=<Kennwort>
```

SCHUTZPARAMETER EXPORTIEREN

Befehlssyntax:

```
avp.com EXPORT <Profil> <Dateiname>
```

Eine Beschreibung der Parameter für die Befehlsausführung ist in der nachstehenden Tabelle zu finden.

<Profil>	Komponente oder Aufgabe, für die der Export von Parametern ausgeführt wird. Als Wert des Parameters **<Profil>** kann ein beliebiger Wert dienen, der im Hilfeabschnitt "Steuerung von Komponenten und Aufgaben des Programms" genannt wird.
<Dateiname>	Pfad der Datei, in welche die Parameter von Kaspersky Internet Security exportiert werden. Ein absoluter oder relativer Pfad kann angegeben werden. Die Konfigurationsdatei wird im Binärformat (dat) gespeichert und kann künftig verwendet werden, um die Einstellungen des Programms auf andere Computer zu übertragen. Außerdem können Sie die Konfigurationsdatei im Textformat speichern. Geben Sie dazu im Dateinamen die Endung txt an. Beachten Sie, dass der Import von Schutzparametern aus einer Textdatei nicht unterstützt wird. Diese Datei kann nur zur Ansicht der grundlegenden Funktionsparameter von Kaspersky Internet Security verwendet werden.

Beispiel:

```
avp.com EXPORT RTP c:\settings.dat
```

SCHUTZPARAMETER IMPORTIEREN

Befehlssyntax:

```
avp.com IMPORT <Dateiname> [/password=<Kennwort>]
```

Eine Beschreibung der Parameter für die Befehlsausführung ist in der nachstehenden Tabelle zu finden.

<Dateiname>	Pfad der Datei, aus welcher die Parameter von Kaspersky Internet Security importiert werden. Ein absoluter oder relativer Pfad kann angegeben werden.
<Kennwort>	Kennwort für Kaspersky Internet Security, das über die Programmoberfläche festgelegt wurde. <Kennwort>

Beachten Sie, dass dieser Befehl nicht ausgeführt wird, wenn das Kennwort nicht eingegeben wird.

Beispiel:

```
avp.com IMPORT c:\settings.dat /password=<Ihr_Kennwort>
```

PROTOKOLLDATEI ANLEGEN

Das Anlegen einer Protokolldatei kann erforderlich sein, wenn bei der Arbeit von Kaspersky Internet Security Probleme auftreten. Die Protokolldatei ermöglicht den Experten des Technischen Supports eine genaue Problemanalyse.

Es wird empfohlen, das Anlegen von Tracing-Dateien nur zur Diagnose eines konkreten Problems zu aktivieren. Sollte das Tracing ständig aktiv sein, so kann die Leistungsfähigkeit des Computers sinken und es kann zur Überfüllung der Festplatte kommen.

Befehlssyntax:

```
avp.com TRACE [file] [on|off] [<Tracing-Niveau>]
```

Folgende Tabelle beschreibt die Parameter.

[on|off]	Anlegen einer Protokolldatei aktivieren / deaktivieren.
[file]	Tracing in Form einer Datei erstellen.
<Tracing-Niveau>	Für diesen Parameter kann ein Zahlenwert im Bereich von 0 (minimale Stufe, nur kritische Meldungen) bis 700 (maximale Stufe, alle Meldungen) festgelegt werden. Wenn Sie sich an den Technischen Support wenden, nennt Ihnen der zuständige Spezialist das erforderliche Tracing-Niveau. Andernfalls gilt das Niveau 500 als empfehlenswert.

Beispiele:

- *Erstellen von Protokolldateien deaktivieren:*

```
avp.com TRACE file off
```

- *Erstellen einer Tracing-Datei zum Senden an den Technischen Support, mit einem maximalen Tracing-Niveau von 500:*

```
avp.com TRACE file on 500
```

HILFE ANZEIGEN

Folgender Befehl dient zur Anzeige von Hilfeinformationen über die Syntax der Befehlzeile:

```
avp.com [ /? | HELP ]
```

Um Hilfeinformationen über die Syntax eines konkreten Befehls zu erhalten, können Sie einen der folgenden Befehle verwenden:

```
avp.com <Befehl> /?
avp.com HELP <Befehl>
```

RÜCKGABECODES DER BEFEHLSZEILE

In diesem Abschnitt werden die Rückgabecodes der Befehlszeile beschrieben (s. folgende Tabelle). Die allgemeinen Codes können von einem beliebigen Befehl der Befehlszeile zurückgegeben werden. Als Rückgabecodes für Aufgaben sind die allgemeinen Codes sowie spezifische Codes für einen konkreten Aufgabentyp möglich.

ALLGEMEINE RÜCKGABECODES	
0	Operation wurde erfolgreich ausgeführt
1	Ungültiger Parameterwert
2	Unbekannter Fehler
3	Fehler bei Ausgabenausführung
4	Aufgabenausführung wurde abgebrochen
RÜCKGABECODES FÜR AUFGABEN ZUR VIRENSUCHE	
101	Alle gefährlichen Objekte wurden bearbeitet
102	Es wurden gefährliche Objekte gefunden

GLOSSAR

2

2-CHANNEL-GATEWAY

Computer mit zwei Netzwerkadaptern, die an verschiedene Netzwerke angeschlossen sind und Daten von einem Netzwerk an ein anderes Netzwerk übermitteln.

A

AKTIVE LIZENZ

Lizenz, die momentan für die Arbeit des Kaspersky-Lab-Programms verwendet wird. Die Lizenz legt die Gültigkeitsdauer für den vollen Funktionsumfang sowie die Lizenzpolitik für das Programm fest. Im Programm kann nur ein Schlüssel den Status "aktiv" besitzen.

ALTERNATIVE NTFS-DATENSTRÖME

Datenströme des NTFS-Dateisystems (alternate data streams), die für zusätzliche Attribute oder Datei-Informationen vorgesehen sind.

Jede Datei im NTFS-Dateisystem stellt eine Auswahl von Datenströmen (streams) dar. In einem Datenstrom befindet sich der Datei-Inhalt, den man sehen kann, wenn man die Datei öffnet, die übrigen (alternativen) Datenströme sind für Meta-Informationen vorgesehen und bieten zum Beispiel die Kompatibilität des NTFS-Systems mit anderen Systemen, wie mit dem alten Dateisystem von Macintosh - Hierarchical File System (HFS). Die Datenströme lassen sich erstellen, löschen, separat speichern, umbenennen und sogar als Prozess starten.

Alternative Datenströme können von Angreifern missbraucht werden, um Daten des Computers heimlich zu übertragen oder zu empfangen.

ANSTÖßIGE E-MAIL

Nachricht, die anstößige Ausdrücke enthält.

ARCHIV

Datei, die ein oder mehrere Objekte "enthält", die ihrerseits auch Archive sein können.

AUFGABE

Funktionen, die das Kaspersky-Lab-Programm ausführen kann und die als Aufgaben realisiert sind, Beispiele: Echtzeitschutz für Dateien, Vollständige Untersuchung des Computers, Datenbank-Update.

AUFGABENEINSTELLUNGEN

Parameter für die Arbeit des Programms, die für jeden Aufgabentyp individuell sind.

AUSNAHME

Eine Ausnahme ist ein Objekt, das von der Untersuchung durch das Kaspersky-Lab-Programm ausgeschlossen wird. Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte nach einem Bedrohungstyp gemäß der Klassifikation der Viren-Enzyklopädie ausgeschlossen werden. Für jede Aufgabe können individuelle Ausnahmen festgelegt werden.

AUTOSTART-OBJEKTE

Auswahl von Programmen, die für den Start und die korrekte Funktion des auf Ihrem Computer installierten Betriebssystems und der vorhandenen Software erforderlich sind. Diese Objekte werden jedes Mal beim Hochfahren des Betriebssystems gestartet. Es gibt Viren, die speziell diese Objekte infizieren können. Dadurch kann beispielsweise das Hochfahren des Betriebssystems blockiert werden.

B

BENACHRICHTIGUNGSVORLAGE

Vorlage, mit der bei der Untersuchung erkannte infizierte Objekte gemeldet werden. Eine Benachrichtigungsvorlage enthält mehrere Einstellungen, die die Reihenfolge der Benachrichtigung, die Verbreitungsart und den Meldungstext definieren.

BOOTVIRUS

Virus, der die Bootsektoren von Computerlaufwerken infiziert. Der Virus "zwingt" das System beim Hochfahren, nicht auf den eigentlichen Bootcode zuzugreifen, sondern auf den Viruscode, der dann die Kontrolle übernimmt.

D

DATEIMASKE

Platzhalter für den Namen und die Erweiterung einer Datei, der aus allgemeinen Zeichen besteht. Die zwei wichtigsten Zeichen, die in Dateimasken verwendet werden sind * und ? (wobei * für eine beliebige Anzahl von beliebigen Zeichen und ? für ein beliebiges Einzelzeichen steht). Mit Hilfe dieser Zeichen kann jede beliebige Datei dargestellt werden. Beachten Sie, dass Name und Endung einer Datei stets durch einen Punkt getrennt werden.

DATENBANK FÜR PHISHING-WEBADRESSEN

Eine Liste der Webressourcen, die von den Kaspersky-Lab-Spezialisten als Phishing-Adressen eingestuft wurden. Die Datenbank wird regelmäßig aktualisiert und gehört zum Lieferumfang des Kaspersky-Lab-Programms.

DATENBANK FÜR VERDÄCHTIGE WEBADRESSEN

Eine Liste der Webressourcen, deren Inhalt als potentiell gefährlich eingestuft werden kann. Die Liste ist von den Kaspersky-Lab-Spezialisten angelegt, wird regelmäßig aktualisiert und gehört zum Lieferumfang des Programms.

DATENBANK-UPDATE

Eine Funktion, die vom Kaspersky-Lab-Programm ausgeführt wird und die es erlaubt, den aktuellen Zustand des Schutzes aufrecht zu erhalten. Dabei werden die Datenbanken von den Kaspersky-Lab-Updateservern auf den Computer kopiert und automatisch von der Anwendung übernommen.

DATENBANKEN

Datenbanken, die von den Kaspersky-Lab-Spezialisten gepflegt werden und eine genaue Beschreibung aller momentan existierenden Bedrohungen der Computersicherheit sowie Methoden zu ihrer Identifikation und Desinfektion enthalten. Die Datenbanken werden von Kaspersky Lab laufend aktualisiert, wenn neue Bedrohungen auftauchen.

DESINFEKTION VON OBJEKTEN

Methode zur Bearbeitung von infizierten Objekten, bei der die Daten vollständig oder teilweise wiederhergestellt werden oder eine Entscheidung darüber getroffen wird, dass die Desinfektion von Objekten nicht möglich ist. Die Desinfektion von Objekten erfolgt auf Basis der Einträge in den Datenbänken. Bei der Desinfektion können Daten teilweise verloren gehen.

DESINFEKTION VON OBJEKTEN BEIM NEUSTART

Methode zur Verarbeitung von infizierten Objekten, die im Augenblick der Desinfektion von anderen Programmen verwendet werden. Dabei wird eine Kopie des infizierten Objekts angelegt. Beim folgenden Neustart wird die Kopie desinfiziert und das infizierte Originalobjekt wird durch die desinfizierte Kopie ersetzt.

DOMAIN NAME SERVICE (DNS)

Verbreitetes System zur Umformung von Hostnamen (Computer oder anderes Netzwerkgerät) in eine IP-Adresse. DNS funktioniert in TCP/IP-Netzwerken. Im Einzelfall kann DNS auch umgekehrte Anfragen und Definitionen von Hostnamen nach dessen IP (PTR-Eintrag) speichern und verarbeiten. Die Auflösung von DNS-Namen erfolgt gewöhnlich durch Netzwerkprogramme und nicht durch die Benutzer.

DRINGENDES UPDATE

Kritisches Update für die Module des Kaspersky-Lab-Programms.

E

E-MAIL LÖSCHEN

Verarbeitungsmethode für eine E-Mail, bei der die Nachricht physikalisch gelöscht wird. Diese Methode wird für E-Mails empfohlen, die eindeutig Spam oder ein schädliches Objekt enthalten. Vor dem Löschen einer Nachricht, wird ihre Kopie im Backup gespeichert (wenn diese Funktion nicht deaktiviert wurde).

ECHTZEITSCHUTZ

Funktionsmodus des Programms, in dem Objekte im Echtzeitmodus auf schädlichen Code untersucht werden.

Das Programm fängt jeden Versuch zum Öffnen, Schreiben und Ausführen eines Objekts ab, und durchsucht das Objekt nach Bedrohungen. Virenfreie Objekte werden für den Zugriff freigegeben, infizierte oder verdächtige Objekte werden gemäß den Aufgabenparametern verarbeitet (desinfiziert, gelöscht, in die Quarantäne verschoben).

EIN- UND AUSGABEPORT

Wird in Mikroprozessoren (z.B. Intel) beim Datenaustausch mit der Hardware verwendet. Der Ein- und Ausgabeport wird einem bestimmten Gerät zugeordnet und erlaubt es den Programmen, zum Datenaustausch darauf zuzugreifen.

EMPFOHLENE STUFE

Sicherheitsstufe, deren Funktionsparameter von Kaspersky Lab empfohlen werden und die einen optimalen Schutz Ihres Computers gewährleistet. Diese Stufe wird in der Grundeinstellung verwendet.

F

FEHLALARM

Situation, in der ein virenfreies Objekt von der Kaspersky-Lab-Anwendung als infiziert eingestuft wird, weil sein Code Ähnlichkeit mit einem Virus aufweist.

G

GEFÄHRLICHES OBJEKT

Objekt, in dem sich ein Virus befindet. Es wird davor gewarnt, mit solchen Objekten zu arbeiten, weil dies zur Infektion des Computers führen kann. Beim Fund eines infizierten Objekts wird empfohlen, das Objekt mit Hilfe des Kaspersky-Lab-Programms zu desinfizieren oder, falls die Desinfektion nicht möglich ist, es zu löschen.

GEPACKTE DATEI

Archivdatei, die ein Extrahierprogramm und für das Betriebssystem bestimmte Extrahierbefehle enthält.

GÜLTIGKEITSDAUER DER LIZENZ

Zeitraum, für den Sie berechtigt sind, das Kaspersky-Lab-Programm mit allen Funktionen zu nutzen. Die Gültigkeitsdauer der Lizenz beträgt in der Regel ein Kalenderjahr ab der Installation der Lizenz. Wenn die Gültigkeitsdauer der Lizenz abgelaufen ist, wird die Funktionalität des Programms eingeschränkt: Das Update der Datenbanken ist nicht mehr verfügbar.

H

HARDWARE-PORT

Eingang an einem Hardware-Element des Computers, an den ein Kabel oder ein Stecker angeschlossen werden kann (LPT-Port, serieller Port, USB).

HEURISTISCHE ANALYSE

Technologie zum Erkennen von Bedrohungen, die nicht mit Hilfe der Datenbanken für Kaspersky-Lab-Programme identifiziert werden können. Es wird erlaubt, Objekte zu finden, die verdächtig sind, durch einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus infizierte zu sein.

Mit Hilfe der heuristischen Analyse werden bis zu 92 % der neuen Bedrohungen erkannt. Dieser Mechanismus ist sehr effektiv und führt nur selten zu einem Fehlalarm.

Dateien, die mit Hilfe der heuristischen Analyse gefunden werden, nennt man verdächtig.

I

ICHECKER-TECHNOLOGIE

Diese Technologie erlaubt eine Erhöhung der Untersuchungsgeschwindigkeit. Dabei werden jene Objekte von der Untersuchung ausgeschlossen, die seit dem vorherigen Scannen nicht verändert wurden, wobei vorausgesetzt wird, dass die Untersuchungsparameter (Antiviren-Datenbanken und Einstellungen) gleich geblieben sind. Informationen darüber werden einer speziellen Datenbank aufgezeichnet. Die Technologie wird sowohl für den Echtzeitschutz als auch für den Scan auf Befehl verwendet.

Wurde beispielsweise eine Archivdatei vom Programm untersucht und ihr wurde der Status virenfrei zugewiesen. Dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und die Untersuchungsparameter gleich geblieben sind. Wenn seit der letzten Untersuchung die Zusammensetzung des Archivs durch Hinzufügen eines neuen Objekts verändert wurde, die Untersuchungsparameter geändert oder die Programm-Datenbanken aktualisiert wurden, wird das Archiv erneut untersucht.

Einschränkungen der Technologie iChecker:

- Die Technologie funktioniert nicht mit großen Dateien, da die Untersuchung der gesamten Datei in diesem Fall weniger Zeit beansprucht, als zu ermitteln, ob sie seit der letzten Untersuchung verändert wurde.
- Die Technologie unterstützt eine begrenzte Anzahl von Formaten (**exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar**).

INDIKATOR FÜR EINE VIRENEPIDEMIE

Vorlage, auf der eine Benachrichtigung über den drohenden Ausbruch einer Virenepidemie beruht. Der Indikator für eine Virenepidemie umfasst einige Einstellungen, die den Schwellenwert der Virenaktivität, die Verbreitungsart und den Meldungstext enthalten.

INFIZIERTES OBJEKT

Objekt, das schädlichen Code enthält: Bei der Untersuchung des Objekts wurde erkannt, dass ein Abschnitt des Objektcodes vollständig mit dem Code einer bekannten Bedrohung übereinstimmt. Die Kaspersky-Lab-Spezialisten warnen davor, mit solchen Objekten zu arbeiten, weil dies zur Infektion Ihres Computers führen kann.

INKOMPATIBLES PROGRAMM

Antiviren-Programm eines Drittherstellers oder Kaspersky-Lab-Programm, das nicht mit Kaspersky Internet Security verwaltet werden kann.

INSTALLATION MIT LOGIN-SZENARIO

Remote-Installation von Kaspersky-Lab-Programmen, mit der der Start der Aufgabe zur Remote-Installation mit einem konkreten Benutzerkonto (mehreren Benutzerkonten) verknüpft werden kann. Beim Anmelden des Benutzers in der Domäne wird versucht, das Programm auf dem Client-Computer zu installieren, auf dem sich der Benutzer angemeldet hat. Dieses Verfahren wird für die Installation von Programmen des Herstellers auf Computern mit den Betriebssystemen Microsoft Windows 98 / Me empfohlen.

INTERCEPTOR

Subkomponente des Programms, die für die Untersuchung bestimmter Typen von E-Mails verantwortlich ist. Die Auswahl der zu installierenden Interceptoren ist davon abhängig, in welcher Rolle oder Rollenkombination das Programm eingesetzt werden soll.

INTERNETPROTOKOLL (IP)

Basisprotokoll für das Internet, das seit seiner Entwicklung im Jahre 1974 unverändert verwendet wird. Es führt die Grundoperationen bei der Datenübertragung von einem Computer auf einen anderen aus und dient als Basis für alle Protokolle höherer Ebenen wie TCP und UDP. Es kontrolliert die Verbindung und die Fehlerbehandlung. Technologien wie IPv4 und Maskierung ermöglichen es, umfangreiche Netzwerke hinter einer relativ geringen Anzahl von IP-Adressen zu verbergen (oder sogar hinter einer Adresse). Dadurch wird erlaubt, die Ansprüche des ständig expandierenden Internets unter Verwendung eines relativ begrenzten IPv4-Adressraums zu befriedigen.

K

KASPERSKY SECURITY NETWORK

Kaspersky Security Network (KSN) ist eine Infrastruktur der Online-Dienste und -Services, die den Zugriff auf die aktuelle Wissensdatenbank von Kaspersky Lab über den "Ruf" der Dateien, Internet-Ressourcen und Programme bietet. Durch die Verwendung der Daten von Kaspersky Security Network wird die Geschwindigkeit der Reaktion von Kaspersky Internet Security auf neue Bedrohungen und die Leistungsfähigkeit einiger Komponenten erhöht. Außerdem wird dadurch das Risiko verringert, dass Fehlalarme auftreten.

KASPERSKY-LAB-UPDATESERVER

Liste der HTTP- und FTP-Server von Kaspersky Lab, von denen das Programm die Updates für Datenbanken und Module auf Ihren Computer herunterlädt.

KONTROLLIERTES OBJEKT

Datei, die mit den Protokollen HTTP, FTP oder SMTP übertragen und von der Firewall zur Untersuchung durch das Kaspersky-Lab-Programm umgeleitet wird.

KOPFZEILE (HEADER)

Informationen, die am Anfang einer Datei oder E-Mail stehen und Basisdaten über Status und Verarbeitung der Datei (E-Mail) enthalten. Die Kopfzeile einer E-Mail enthält z.B. Angaben über Absender, Empfänger und Datum.

L

LAUFWERKSBOOTSEKTOR

Ein Bootsektor ist ein spezieller Sektor auf der Festplatte eines Computers, auf einer Diskette oder auf einem anderen Gerät zur Datenspeicherung. Er enthält Angaben über das Dateisystem des Datenträgers und ein Bootprogramm, das für den Start des Betriebssystems verantwortlich ist.

Laufwerksbootsektoren können von so genannten Bootviren infiziert werden. Die Kaspersky-Lab-Anwendung erlaubt es, Bootsektoren auf Viren zu untersuchen und infizierte Sektoren zu desinfizieren.

LISTE DER VERTRAUENSWÜRDIGEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, deren Inhalt der Benutzer vertraut. Webseiten, die einem Element dieser Liste entsprechen, werden vom Kaspersky-Lab-Programm auf das Vorhandensein schädlicher Objekte nicht untersucht.

LISTE DER ZU UNTERSUCHENDEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, die vom Kaspersky-Lab-Programm auf das Vorhandensein schädlicher Objekte unbedingt untersucht werden sollen.

LISTE MIT ERLAUBTEN ABSENDERN

(auch weiße Adressenliste)

Liste mit E-Mail-Adressen. Die von diesen Adressen eintreffenden Nachrichten werden nicht vom Kaspersky-Lab-Programm untersucht.

LISTE MIT ERLAUBTEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, auf die der Zugriff vom Kaspersky-Lab-Programm nicht blockiert wird. Eine Adressenliste wird vom Benutzer bei der Programmkonfiguration erstellt.

LISTE MIT VERBOTENEN ABSENDERN

(auch schwarze Adressenliste)

Liste mit E-Mail-Adressen. Die von diesen Adressen eintreffenden Nachrichten werden vom Kaspersky-Lab-Programm ungeachtet ihres Inhalts blockiert .

LISTE MIT VERBOTENEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, auf die der Zugriff vom Kaspersky-Lab-Programm blockiert wird. Eine Adressenliste wird vom Benutzer bei der Programmkonfiguration erstellt.

M

MAIL-DATENBANKEN

Datenbanken mit einem speziellen Format, in denen die auf Ihrem Computer gespeicherten E-Mails enthalten sind. Jede eingehende / ausgehende E-Mail wird nach dem Empfang / Senden in einer Mail-Datenbank gespeichert. Solche Datenbanken werden bei einer vollständigen Untersuchung des Computers untersucht.

Eingehende und ausgehende E-Mails werden im Augenblick des Empfangs und Sendens in Echtzeit auf Viren analysiert, wenn der Echtzeitschutz aktiviert ist.

MÖGLICHERWEISE INFIZIERTES OBJEKT

Objekt, dessen Code entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus gleicht, enthält, der Kaspersky Lab aber bisher nicht bekannt ist. Infizierte Dateien können mit Hilfe der heuristischen Analyse gefunden werden.

N

NETZWERKPORT

Parameter für die Protokolle TCP und UDP, der den Zweck von Datenpaketen im IP-Format definiert, die über ein Netzwerk auf einen Host übertragen werden. Er erlaubt unterschiedlichen auf einem Host ausgeführten Programmen, unabhängig voneinander Daten zu empfangen. Jedes Programm verarbeitet die Daten, die auf einem bestimmten Port eintreffen (man sagt auch, ein Programm "hört" einen bestimmten Port).

Gewöhnlich sind häufig verwendeten Netzwerkprotokollen standardmäßige Portnummern zugeordnet (Webserver empfangen ihre Daten standardmäßig mit dem HTTP-Protokoll auf TCP-Port 80), obwohl ein Programm prinzipiell ein beliebiges Protokoll und einen beliebigen Port verwenden kann. Mögliche Werte: von 1 bis 65535.

O

OLE-OBJEKT

Objekt, das an eine andere Datei angehängt oder darin eingebettet ist. Das Kaspersky-Lab-Programm erlaubt es, OLE-Objekte auf das Vorhandensein von Viren zu untersuchen. Wenn Sie beispielsweise eine beliebige Tabelle aus Microsoft Office Excel in ein Dokument des Typs Microsoft Office Word einfügen, wird die Tabelle als OLE-Objekt untersucht.

OBJEKT BLOCKIEREN

Der Zugriff externer Programme auf ein Objekt wird verboten. Ein blockiertes Objekt kann nicht gelesen, ausgeführt, verändert oder gelöscht werden.

OBJEKT LÖSCHEN

Methode zur Objektbearbeitung, bei der das Objekt physikalisch von dem Ort gelöscht wird, an dem es vom Programm gefunden wurde (Festplatte, Ordner, Netzwerkressource). Diese Bearbeitungsmethode wird für gefährliche Objekte empfohlen, deren Desinfektion aus bestimmten Gründen nicht möglich ist.

OBJEKTE IN DIE QUARANTÄNE VERSCHIEBEN

Verarbeitungsmethode für ein möglicherweise infiziertes Objekt. Dabei wird der Zugriff auf das Objekt gesperrt und das Objekt wird vom ursprünglichen Speicherort in den Quarantäneordner verschoben. Dort wird es in verschlüsselter Form gespeichert, um eine Infektion auszuschließen.

P

PHISHING

Eine Art des Internetbetrugs, bei der E-Mails verschickt werden, um vertrauliche Informationen (i.d.R. finanziellen Charakters) zu stehlen.

POTENTIELL INFIZIERBARES OBJEKT

Ein Objekt das aufgrund seiner Struktur seines Formats von einem Angreifer als "Container" benutzt werden kann, um ein schädliches Objekt zu platzieren oder weiterzuverbreiten. In der Regel sind dies ausführbare Dateien mit Erweiterungen wie com, exe, dll usw. Das Risiko des Eindringens und der Aktivierung von schädlichem Code ist für solche Dateien relativ hoch.

PRIORITÄTSSTUFE FÜR EIN EREIGNIS

Merkmale eines Ereignisses, das bei der Arbeit der Kaspersky-Lab-Anwendung eingetreten ist. Es gibt vier Prioritätsstufen:

- **Kritisches Ereignis**.
- **Funktionsstörung**.
- **Warnung**.
- **Informative Meldung**.

Ereignisse des gleichen Typs können unterschiedliche Prioritätsstufen besitzen. Entscheidend ist die Situation, in der ein Ereignis eintritt.

PROGRAMM AKTIVIEREN

Freischalten aller Programmfunktionen. Für die Aktivierung des Programms benötigt der Benutzer eine Lizenz.

PROGRAMM-MODULE

Dateien, die zum Lieferumfang von Kaspersky Lab gehören und für die Realisierung der wichtigsten Aufgaben zuständig sind. Jeder Art von Aufgaben, die das Programm realisiert (Echtzeitschutz, Virensuche, Update), entspricht ein eigenes ausführbares Modul. Wenn die vollständige Untersuchung Ihres Computers aus dem Hauptfenster gestartet wird, initiieren Sie den Start des Moduls für diese Aufgabe.

PROGRAMMEINSTELLUNGEN

Einstellungen für die Arbeit des Programms, die für alle Aufgabentypen gleich sind und sich auf das gesamte Programm beziehen (z.B. Leistungseinstellungen für das Programm, Einstellungen für das Berichtswesen, Backup-Einstellungen).

PROTOKOLL

Genau definierte und standardisierte Kombination von Regeln, die das Verhältnis zwischen Client und Server regulieren. Bekannte Protokolle und die entsprechenden Dienste sind z.B. HTTP (WWW), FTP und NNTP (News).

PROXYSERVER

Dienst in Computernetzwerken, mit dem Clients indirekte Anfragen an andere Netzwerkdienste richten können. Zunächst baut der Client eine Verbindung zu einem Proxyserver auf und fragt nach einer bestimmten Ressource (zum Beispiel nach einer Datei), die auf einem anderen Server liegt. Dann stellt der Proxyserver mit dem angegebenen Server eine Verbindung her und nimmt von ihm die Ressource entgegen oder schreibt die Ressource in seinen eigenen Cache (falls der Proxy einen Cache besitzt). In einigen Fällen kann die Client-Anfrage oder Server-Antwort vom Proxyserver zu bestimmten Zwecken geändert werden.

Q

QUARANTÄNE

Ein bestimmter Ordner, in den alle möglicherweise infizierten Objekte verschoben werden, die bei der Untersuchung oder im Rahmen des Echtzeitschutzes gefunden werden.

R

RESERVELIZENZ

Lizenz, die für die Arbeit der Kaspersky-Lab-Anwendung hinzugefügt, aber nicht aktiviert wurde. Eine Reservelizenz wird aktiviert, wenn die Gültigkeit der aktiven Lizenz abläuft.

RISIKOBEWERTUNG

Kennziffer für das Risiko, das ein Computerprogramm für das Betriebssystem darstellt. Die Bewertung erfolgt durch eine heuristische Analyse, die auf zweierlei Kriterien beruht:

- statische Kriterien (z.B. Informationen über die ausführbare Programmdatei: Dateigröße, Erstellungsdatum usw.)
- dynamische Kriterien, die dazu dienen, um die Arbeit des Programms in einer virtuellen Umgebung zu modellieren (Analyse der Aufrufe von Systemfunktionen durch das Programm).

Die Risikobewertung erlaubt es, für Schadprogramme typisches Verhalten zu erkennen. Je niedriger die Risikobewertung, desto mehr Aktionen werden einem Programm im System erlaubt.

S

SOCKS

Proxyserver-Protokoll, mit dem eine zweiseitige Verbindung zwischen Computern eines lokalen und externen Netzwerks realisiert werden kann.

SCHLÜSSELDATEI

Datei mit der Endung .key, die Ihr persönlicher "Schlüssel" ist und für die Arbeit des Kaspersky-Lab-Programms erforderlich ist. Eine Schlüsseldatei ist im Lieferumfang des Produkts enthalten, wenn es bei einem Händler von Kaspersky Lab erworben wurde, oder Sie erhalten sie per E-Mail, wenn das Produkt in einem Internet-Shop gekauft wurde.

SCHUTZSTATUS

Aktueller Schutzstatus, der das Sicherheitsniveau des Computers charakterisiert.

SCHWARZE LISTE FÜR SCHLÜSSELDATEIEN

Datenbank mit Informationen über die von Kaspersky Lab blockierten Schlüsseldateien. Die Datei mit der Schwarzen Liste wird gemeinsam mit den Datenbanken aktualisiert.

SCHWELLE FÜR VIRENAKTIVITÄT

Maximal zulässige Anzahl von Ereignissen eines bestimmten Typs innerhalb eines festgelegten Zeitraums, deren Überschreitung als erhöhte Virenaktivität und als Anzeichen eines Virenangriffs gilt. Dieser Wert besitzt insbesondere bei

Viren-Epidemien große Bedeutung und erlaubt es dem Administrator, rechtzeitig auf drohende Virenangriffe zu reagieren.

SICHERHEITSSTUFE

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Parametern für die Arbeit einer Komponente verstanden.

SKRIPT

Ein kleines Computerprogramm oder ein unabhängiger Programmteil (Funktion), das/der in der Regel dazu dient, eine konkrete Aufgabe auszuführen. Meistens werden sie bei Programmen, die in Hypertext integriert sind, verwendet. Skripts werden beispielsweise gestartet, wenn Sie eine bestimmte Webseite öffnen.

Wenn der Echtzeitschutz aktiviert ist, überwacht die Anwendung den Start von Skripts, fängt sie ab und untersucht diese auf Viren. Abhängig von den Untersuchungsergebnissen können Sie die Ausführung eines Skripts verbieten oder erlauben.

SPAM

Unerwünschte massenhafte Versendung von E-Mails, die meistens Werbung enthalten.

SUBNETZMASKE

Die Subnetzmaske (auch Netzwerkmaske genannt) und die Netzwerkadresse definieren die Adressen der Computer, die zu einem Netzwerk gehören.

U

UND

UNBEKANNTER VIRUS

Neuer Virus, über den noch keine Informationen in den Datenbanken vorhanden sind. Unbekannte Viren werden mit der heuristischen Analyse erkannt und erhalten den Status möglicherweise infiziert.

UNTERSUCHUNG DES DATENVERKEHRS

Untersuchung von Objekten, die mit beliebigen Protokollen übertragen werden (z.B. HTTP, FTP u.a.). Die Untersuchung erfolgt im Echtzeitmodus unter Verwendung der aktuellen (letzten) Datenbankversion.

UPDATE

Vorgang, bei dem vorhandene Dateien (Datenbanken oder Programm-Module) durch neue Dateien ersetzt bzw. neue Dateien hinzugefügt werden. Die neuen Dateien werden von den Kaspersky-Lab-Updateservern heruntergeladen.

UPDATEPAKET

Dateipaket, das der Softwareaktualisierung dient, aus dem Internet kopiert und auf Ihrem Computer installiert wird.

V

VERDÄCHTIGE E-MAIL

E-Mail, die sich nicht eindeutig als Spam einstufen lässt, bei deren Untersuchung sich aber ein Verdacht ergeben hat (z.B. bestimmte Arten von Massenmails und Werbenachrichten).

VERDÄCHTIGES OBJEKT

Objekt, dessen Code entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus gleicht, enthält, der Kaspersky Lab aber bisher nicht bekannt ist. Verdächtige Objekte werden unter Einsatz der heuristischen Analyse erkannt.

VERFÜGBARES UPDATE

Updatepaket für die Module eines Kaspersky-Lab-Programms, das dringende Updates, die über einen bestimmten Zeitraum gesammelt wurden, sowie Änderungen der Programmarchitektur enthält.

VERTRAUENSWÜRDIGER PROZESS

Programmprozess, dessen Dateioperationen im Echtzeitschutz nicht von der Kaspersky-Lab-Anwendung kontrolliert werden. Das bedeutet, dass alle von einem vertrauenswürdigen Prozess gestarteten, geöffneten und gespeicherten Objekte nicht untersucht werden.

VIRENANGRIFF

Eine Reihe zielgerichteter Versuche, einen Computer mit einem Virus zu infizieren.

W

WIEDERHERSTELLUNG

Ein Originalobjekt wird aus der Quarantäne oder aus dem Backup entweder an den ursprünglichen Ort, an dem das Objekt gespeichert war, bevor es in die Quarantäne verschoben, desinfiziert oder gelöscht wurde, oder in einen benutzerdefinierten Ordner verschoben.

Z

ZERTIFIKAT DES ADMINISTRATIONSSERVERS

Zertifikat, mit dem der Administrationsserver beim Herstellen einer Verbindung mit der Administrationskonsole und Datenaustausch mit den Client-Computern authentifiziert wird. Das Zertifikat des Administrationsservers wird bei Installation des Administrationsservers angelegt und im Unterordner Cert des Installationsverzeichnisses gespeichert.

KASPERSKY LAB

Kaspersky Lab wurde 1997 gegründet. Heute sind wir das bekannteste Unternehmen für Datenschutz-Software in Russland und bieten eine breite Palette an: Programmen zum Schutz vor Viren, unerwünschten E-Mails (Spam) und Hackerangriffen.

Kaspersky Lab ist ein international operierender Konzern. Die Zentrale befindet sich in Russland, es gibt Niederlassungen in Großbritannien, Frankreich, Deutschland, Japan, in den Benelux-Ländern, China, Polen, Rumänien und in den USA (Kalifornien). In Frankreich wurde eine neue Tochtergesellschaft gegründet, das Europäische Zentrum für Antiviren-Forschung. Unser Partnernetzwerk vereint weltweit mehr als 500 Unternehmen.

Kaspersky Lab – das sind heute mehr als tausend hoch qualifizierte Fachleute, von denen ein Dutzend MBA-Diplome und sechzehn einen Doktortitel besitzen. Die führenden Virusanalytiker von Kaspersky Lab gehören zur prestigeträchtigen Computer Anti-virus Researcher's Organization (CARO).

Das größte Kapital des Unternehmens sind das einzigartige Wissen und die Erfahren, die die Mitarbeiter im Laufe des mehr als vierzehnjährigen ununterbrochenen Kampfes gegen Viren gesammelt haben. Dank der ständigen Analyse von Virenaktivitäten können wir Tendenzen bei der Malware-Entwicklung vorhersagen und frühzeitig Benutzern einen zuverlässigen Schutz vor neuen Angriffen an die Hand geben. Dieser einzigartige Vorteil bildet die Basis der Produkte und Dienstleistungen von Kaspersky Lab. Wir sind unseren Wettbewerbern stets einen Schritt voraus und bieten unseren Kunden den besten Schutz.

Aufgrund der jahrelangen Tätigkeit wurde das Unternehmen zum führenden Entwickler von Technologien zum Schutz vor Viren. Kaspersky Lab hat als erstes Unternehmen viele moderne Standards für Antiviren-Software gesetzt. Die Basis-Software des Unternehmens heißt Kaspersky Anti-Virus und sie sorgt für einen zuverlässigen Schutz aller Objekte vor Virenangriffen: Arbeitsstationen, Dateiserver, Mail-Systeme, Firewalls und Internet-Gateways sowie Taschencomputer. Bequeme Steuerelemente versetzen die Benutzer in die Lage, den Antivirenschutz von Computern und Unternehmensnetzwerken maximal zu automatisieren. Viele internationale Developer verwendeten in ihrer Software den Kernel von Kaspersky Anti-Virus, beispielsweise: Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Die Kunden von Kaspersky Lab kommen in den Genuss eines breiten Spektrums von Zusatzleistungen, die das störungsfreie Funktionieren der Erzeugnisse und die genaue Kompatibilität mit speziellen Business-Vorgaben garantieren. Wir projektieren, realisieren und begleiten Antiviren-Komplex-Lösungen von Unternehmen. Unsere Datenbanken werden stündlich aktualisiert. Wir haben für unsere Benutzer einen technischen Kundendienst in mehreren Sprachen eingerichtet.

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir beraten Sie gern detailliert über das Telefon oder E-Mail. Auf Ihre Fragen bekommen Sie eine vollständige und erschöpfende Antwort.

Webseite von Kaspersky Lab:	http://www.kaspersky.de
Viren-Enzyklopädie:	http://www.securelist.com/de/
Antiviren-Labor:	newvirus@kaspersky.com (nur zum Einsenden verdächtiger Objekte, die zuvor archiviert wurden) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de (für Fragen an die Virenanalytiker)
Webforum von Kaspersky Lab:	http://forum.kaspersky.com

INFORMATIONEN ZUM CODE VON DRITTHERSTELLERN

Bei der Entwicklung des Programms wurde der Code von Drittherstellern verwendet.

In diesem Abschnitt

Programmcode 252

Entwicklungstools 281

Verteilter Programmcode 285

Andere Informationen 294

Programmcode

Bei der Entwicklung des Programms wurde der Programmcode von Drittherstellern verwendet.

IN DIESEM ABSCHNITT

AGG 2.4 254

ADOBE ABI-SAFE CONTAINERS 1.0 255

BOOST 1.39.0 255

BZIP2/LIBBZIP2 1.0.5 255

CONVERTUTF 255

CURL 7.19.4 256

DEELX - REGULAR EXPRESSION ENGINE 1.2 256

EXPAT 1.2, 2.0.1 256

FASTSCRIPT 1.90 257

FDLIBM 5.3 257

FLEX: THE FAST LEXICAL ANALYZER 2.5.4 257

FMT.H 257

GDTOA 257

GECKO SDK 1.8, 1.9, 1.9.1 258

ICU4C 4.0.1 266

INFO-ZIP 5.51 266

JSON4LUA 0.9.30 267

LIBGD 2.0.35 267

LIBJPEG 6B 268

LIBM (lrint.c v 1.4, lrintf.c,v 1.5) 269

LIBPNG 1.2.8, 1.2.9, 1.2.42 270

LIBUNGIF 3.0 270

LIBXDR 270

LREXLIB 2.4 271

LUA 5.1.4 271

LZMALIB 4.43 272

MD5.H 272

MD5.H 272

MD5-CC 1.02 272

OPENSSL 0.9.8K 273

PCRE 7.7, 7.9 274

SHA1.C 1.2 276

STLPORT 5.2.1 276

SVCCTL.IDL 276

TINYXML 2.5.3 276

VISUAL STUDIO CRT SOURCE CODE 8.0 276

WINDOWS TEMPLATE LIBRARY 8.0 277

ZLIB 1.0.4, 1.0.8, 1.2.2, 1.2.3 281

AGG 2.4

Copyright (C) 2002-2005 Maxim Shemanarev (McSeem)

Anti-Grain Geometry has dual licensing model. The Modified BSD License was first added in version v2.4 just for convenience. It is a simple, permissive non-copyleft free software license, compatible with the GNU GPL. It's well proven and recognizable. See http://www.fsf.org/licensing/licenses/index_html#ModifiedBSD for details.

Note that the Modified BSD license DOES NOT restrict your rights if you choose the Anti-Grain Geometry Public License.

Anti-Grain Geometry Public License

Anti-Grain Geometry – Version 2.4

Copyright (C) 2002-2005 Maxim Shemanarev (McSeem)

Permission to copy, use, modify, sell and distribute this software is granted provided this copyright notice appears in all copies. This software is provided "as is" without express or implied warranty, and with no claim as to its suitability for any purpose.

Modified BSD License

Anti-Grain Geometry – Version 2.4

Copyright (C) 2002-2005 Maxim Shemanarev (McSeem)

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

ADOBE ABI-SAFE CONTAINERS 1.0

Copyright (C) 2005, Adobe Systems Incorporated

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVEN SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

BOOST 1.39.0

Copyright (C) 2008, Beman Dawes

BZIP2/LIBBZIP2 1.0.5

Copyright (C) 1996-2007, Julian R Seward

CONVERTUTF

Copyright (C) 2001-2004, Unicode, Inc

Disclaimer

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Limitations on Rights to Redistribute This Code Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

CURL 7.19.4

Copyright (C) 1996-2009, Daniel Stenberg

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2009, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

DEELX - REGULAR EXPRESSION ENGINE 1.2

Copyright (C) 2006, RegExLab.com

http://www.regexlab.com/deelx/

EXPAT 1.2, 2.0.1

Copyright (C) 1998, 1999, 2000, Thai Open Source Software Center Ltd and Clark Cooper

Copyright (C) 2001, 2002, 2003, 2004, 2005, 2006, Expat maintainers

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

FASTSCRIPT 1.90

Copyright (C) Fast Reports Inc

FDLIBM 5.3

Copyright (C) 2004, Sun Microsystems, Inc

Permission to use, copy, modify, and distribute this software is freely granted, provided that this notice is preserved.

FLEX: THE FAST LEXICAL ANALYZER 2.5.4

Copyright (C) 1990, The Regents of the University of California

---

This code is derived from software contributed to Berkeley by Vern Paxson.

The United States Government has rights in this work pursuant to contract no. DE-AC03-76SF00098 between the United States Department of Energy and the University of California.

Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: "This product includes software developed by the University of California, Berkeley and its contributors" in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

FMT.H

Copyright (C) 2002, Lucent Technologies

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR LUCENT TECHNOLOGIES MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

GDTOA

Copyright (C) 1998-2002, Lucent Technologies

Copyright (C) 2004, 2005, 2009, David M. Gay

Copyright (C) 1998-2002, Lucent Technologies

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that the copyright notice and this permission notice and warranty disclaimer appear in supporting documentation, and that the name of Lucent or any of its entities not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

LUCENT DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL LUCENT OR ANY OF ITS ENTITIES BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (C) 2004, 2005, 2009 David M. Gay

Permission to use, copy, modify, and distribute this software and its

documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that the copyright notice and this permission notice and warranty disclaimer appear in supporting documentation, and that the name of the author or any of his current or former employers not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR OR ANY OF HIS CURRENT OR FORMER EMPLOYERS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

GECKO SDK 1.8, 1.9, 1.9.1

Copyright (C) Mozilla Foundation

Mozilla Public License Version 1.1

1. Definitions.

1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

01.08.01. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

01.10.01. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6,1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims: under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

the licenses granted in this Section 2,1 (a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

Notwithstanding Section 2,1 (b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale,

have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

the licenses granted in Sections 2,2 (a) and 2,2 (b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

Notwithstanding Section 2,2 (b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2,2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6,1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3,5.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2,1 or 2,2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3,2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the legal file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3,4 (a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Sections 3,1, 3,2, 3,3, 3,4 and 3,5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3,2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the legal file described in Section 3,4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. Disclaimer of warranty

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

8. Termination

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2,1 and/or 2,2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2,1 and/or 2,2 automatically terminate at the expiration of the 60 day notice period specified above.

any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2,1(b) and 2,2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2,1 or 2,2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8,1 or 8,2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. Limitation of liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall you, the initial developer, any other contributor, or any distributor of covered code, or any supplier of any of such parties, be liable to any person for any indirect, special, incidental, or consequential damages of any character including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to you.

10. U.S. government end users

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48

C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. Miscellaneous

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. Responsibility for claims

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. Multiple-licensed code

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the MPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

Exhibit A - Mozilla Public License.

"The contents of this file are subject to the Mozilla Public License

Version 1.1 (the "License"); you may not use this file except in

compliance with the License. You may obtain a copy of the License at

http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS"

basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the

License for the specific language governing rights and limitations

under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____.

Portions created by _____ are Copyright (C) _____

_____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms

of the _____ license (the "[___] License"), in which case the

provisions of [_____] License are applicable instead of those

above. If you wish to allow use of your version of this file only

under the terms of the [____] License and not to allow others to use

your version of this file under the MPL, indicate your decision by

deleting the provisions above and replace them with the notice and

other provisions required by the [___] License. If you do not delete

the provisions above, a recipient may use your version of this file

under either the MPL or the [___] License."

NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.

AMENDMENTS

The Netscape Public License Version 1.1 ("NPL") consists of the Mozilla Public License Version 1.1 with the following Amendments,

including Exhibit A-Netscape Public License. Files identified with "Exhibit A-Netscape Public License" are governed by the Netscape

Public License Version 1.1.

Additional Terms applicable to the Netscape Public License.

I. Effect.

These additional terms described in this Netscape Public License -- Amendments shall apply to the Mozilla Communicator

client code and to all Covered Code under this License.

II. "Netscape's Branded Code" means Covered Code that Netscape distributes and/or permits others to distribute under one or more trademark(s) which are controlled by Netscape but which are not licensed for use under this License.

III. Netscape and logo.

This License does not grant any rights to use the trademarks "Netscape", the "Netscape N and horizon" logo or the "Netscape

lighthouse" logo, "Netcenter", "Gecko", "Java" or "JavaScript", "Smart Browsing" even if such marks are included in the Original

Code or Modifications.

IV. Inability to Comply Due to Contractual Obligation.

Prior to licensing the Original Code under this License, Netscape has licensed third party code for use in Netscape's Branded Code.

To the extent that Netscape is limited contractually from making such third party code available under this License, Netscape may

choose to reintegrate such code into Covered Code without being required to distribute such code in Source Code form, even if

such code would otherwise be considered "Modifications" under this License.

V. Use of Modifications and Covered Code by Initial Developer.

V.1. In General.

The obligations of Section 3 apply to Netscape, except to the extent specified in this Amendment, Section V.2 and V.3.

V.2. Other Products.

Netscape may include Covered Code in products other than the Netscape's Branded Code which are released by Netscape during the two (2) years following the release date of the Original Code, without such additional products becoming subject to the terms of this License, and may license such additional products on different terms from those contained in this License.

V.3. Alternative Licensing.

Netscape may license the Source Code of Netscape's Branded Code, including Modifications incorporated therein, without such Netscape Branded Code becoming subject to the terms of this License, and may license such Netscape Branded Code on different terms from those contained in this License.

VI. Litigation.

Notwithstanding the limitations of Section 11 above, the provisions regarding litigation in Section 11(a), (b) and (c) of the License shall apply to all disputes relating to this License.

EXHIBIT A-Netscape Public License.

"The contents of this file are subject to the Netscape Public

License Version 1.1 (the "License"); you may not use this file

except in compliance with the License. You may obtain a copy of

the License at http://www.mozilla.org/NPL/

Software distributed under the License is distributed on an "AS

IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or

implied. See the License for the specific language governing

rights and limitations under the License.

The Original Code is Mozilla Communicator client code, released

March 31, 1998.

The Initial Developer of the Original Code is Netscape

Communications Corporation. Portions created by Netscape are

Copyright (C) 1998-1999 Netscape Communications Corporation. All

Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the

terms of the _____ license (the "[___] License"), in which case

the provisions of [_____] License are applicable instead of

those above. If you wish to allow use of your version of this

file only under the terms of the [____] License and not to allow

others to use your version of this file under the NPL, indicate

your decision by deleting the provisions above and replace them

with the notice and other provisions required by the [___]

License. If you do not delete the provisions above, a recipient

may use your version of this file under either the NPL or the

[___] License."

ICU4C 4.0.1

Copyright (C) 1995-2008, International Business Machines Corporation and others

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

INFO-ZIP 5.51

Copyright (C) 1990-2007, Info-ZIP

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided "as is", without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

JSON4LUA 0.9.30

Copyright (C) 2009, Craig Mason-Jones

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBGD 2.0.35

Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Cold Spring Harbor Laboratory. Funded under Grant

P41-RR02188 by the National Institutes of Health.

Portions copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Boutell.Com, Inc.

Portions relating to GD2 format copyright 1999, 2000, 2001, 2002 Philip Warner.

Portions relating to PNG copyright 1999, 2000, 2001, 2002 Greg Roelofs.

Portions relating to gdttf.c copyright 1999, 2000, 2001, 2002 John Ellson (ellson@lucent.com).

Portions relating to gdft.c copyright 2001, 2002 John Ellson (ellson@lucent.com).

Portions copyright 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007 Pierre-Alain Joye (pierre@libgd.org).

Portions relating to JPEG and to color quantization copyright 2000, 2001, 2002, Doug Becker and copyright (C) 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group. See the file README-JPEG.TXT for more information.

Portions relating to WBMP copyright 2000, 2001, 2002 Maurice Szmurlo and Johan Van den Brande.

Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation.

This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user-accessible documentation.

This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation.

Although their code does not appear in gd, the authors wish to thank David Koblas, David Rowley, and Hutchison Avenue Software Corporation for their prior contributions.

LIBJPEG 6B

Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding

LEGAL ISSUES

==========

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)

2. You can use this software for whatever you want. You don't have to pay us.

3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA.

ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable.

The same holds for its supporting scripts (config.guess, config.sub, ltmain.sh). Another support script, install-sh, is copyright by X Consortium but is also freely distributable.

The IJG distribution formerly included code to read and write GIF files.

To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that "The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

LIBM (LRINT.C V 1.4, LRINTF.C,V 1.5)

Copyright (C) 2004, Matthias Drochner

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

LIBPNG 1.2.8, 1.2.9, 1.2.42

Copyright (C) 2004, 2006-2009, Glenn Randers-Pehrson

LIBUNGIF 3.0

Copyright (C) 1997, Eric S. Raymond

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBXDR

Copyright (C) Sun Microsystems, Inc

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part.

Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue

Mountain View, California 94043

LREXLIB 2.4

Copyright (C) 2000-2008, Reuben Thomas Copyright (C) 2004-2008, Shmuel Zeigerman

---

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LUA 5.1.4

Copyright (C) 1994-2008, Lua.org, PUC-Rio

Lua License

Lua is licensed under the terms of the MIT license reproduced below.

This means that Lua is free software and can be used for both academic and commercial purposes at absolutely no cost.

For details and rationale, see http://www.lua.org/license.html .

Copyright (C) 1994-2008 Lua.org, PUC-Rio.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE,

ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LZMALIB 4.43

MD5.H

Copyright (C) 1999, Aladdin Enterprises

MD5.H

Copyright (C) 1990, RSA Data Security, Inc

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

MD5-CC 1.02

Copyright (C) 1991-1992, RSA Data Security, Inc

Copyright (C) 1995, Mordechai T. Abzug

This software contains a C++/object oriented translation and modification of MD5 (version 1.02) by Mordechai T. Abzug. Translation and modification (c) 1995 by Mordechai T. Abzug

Copyright 1991-1992 RSA Data Security, Inc.

The MD5 algorithm is defined in RFC 1321. This implementation is derived from the reference C code in RFC 1321 which is covered by the following copyright statement:

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

OPENSSL 0.9.8K

Copyright (C) 1998-2008, The OpenSSL Project

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

==========

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project

for use in the OpenSSL Toolkit. (http://www.openssl.org/)" 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

PCRE 7.7, 7.9

Copyright (C) 1997-2009, University of Cambridge

Copyright (C) 2007-2008, Google Inc

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 7 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England.

Copyright (c) 1997-2009 University of Cambridge

All rights reserved.

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

Copyright (c) 2007-2008, Google Inc.

All rights reserved.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

End

SHA1.C 1.2

Author Steve Reid (steve@edmweb.com)

STLPORT 5.2.1

Copyright (C) 1994, Hewlett-Packard Company

Copyright (C) 1996-1999, Silicon Graphics Computer Systems, Inc.

Copyright (C) 1997, Moscow Center for SPARC Technology

Copyright (C) 1999-2003, Boris Fomitchev

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

SVCCTL.IDL

Copyright (C) 2010, Microsoft Corporation

TINYXML 2.5.3

Copyright (C) 2000-2006, Lee Thomason

VISUAL STUDIO CRT SOURCE CODE 8.0

Copyright (C) Microsoft Corporation

WINDOWS TEMPLATE LIBRARY 8.0

Copyright (C) Microsoft Corporation

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

ZLIB 1.0.4, 1.0.8, 1.2.2, 1.2.3

Copyright (C) 1995-2010, Jean-loup Gailly and Mark Adler

ENTWICKLUNGSTOOLS

Bei der Entwicklung des Programms wurden die Entwicklungstools und und andere Mittel von Drittherstellern verwendet.

IN DIESEM ABSCHNITT

MS DDK 4.0, 2000 281

MS WDK 6000, 6001, 6002..... 281

WINDOWS INSTALLER XML (WIX) TOOLSET 3.0 281

MS DDK 4.0, 2000

Copyright (C) Microsoft Corporation

MS WDK 6000, 6001, 6002

Copyright (C) 2001-2007, Microsoft Corporation

WINDOWS INSTALLER XML (WIX) TOOLSET 3.0

Copyright (C) Microsoft Corporation

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. DEFINITIONS

"Contribution" means:

a) in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

b) in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE

EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

VERTEILTER PROGRAMMCODE

Mit dem Programm wird ein unabhängiger Programmcode von Drittherstellern in seinem Quell- oder Binärformat ohne Änderungen verbreitet.

IN DIESEM ABSCHNITT

GRUB4DOS 0.4.4-2009-10-16 (FILE GRUB.EXE) 286

SYSLINUX 3.86 (FILE SYSLINUX.EXE) 290

GRUB4DOS 0.4.4-2009-10-16 (FILE GRUB.EXE)

Copyright (C) 1999, 2000, 2001, 2002, 2004, 2005 Free Software Foundation, Inc

---

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of

preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision'

(which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

SYSLINUX 3.86 (FILE SYSLINUX.EXE)

Copyright (C) 1994-2010, H. Peter Anvin et al

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of

preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.  This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision'

(which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

ANDERE INFORMATIONEN

Zusatzinformationen zum Code von Drittherstellern

Zur Überprüfung der elektronischen digitalen Signatur wird die Programmbibliothek für den Informationsschutz (PBSI) "Agava-C" eingesetzt, die von R-Alpha OOO entwickelt wurde.

Die Software kann einige Softwareprogramme enthalten, die an den Nutzer unter der GPL (GNU General Public License) oder sonstigen vergleichbaren freien Softwarelizenzen lizenziert (oder unterlizenziert) sind und dem Nutzer neben anderen Rechten gestatten, bestimmte Programme oder Teile dieser Programme zu kopieren, zu modifizieren und weiter zu verbreiten und sich Zugang zum Quellcode zu verschaffen ("Open Source Software"). Falls es solche Lizenzen erforderlich machen, dass für jedwede Software, die an jemanden in ausführbarem Binärformat geliefert wird, diesen Nutzern der Quellcode ebenfalls verfügbar gemacht wird, dann soll der Quellcode zur Verfügung gestellt werden, indem ein diesbezügliches Ersuchen an source@kaspersky.com gesendet wird, oder der Quellcode wird mit der Software geliefert.

Für die Überprüfung elektronischer digitaler Signaturen wird die Krypto-Bibliothek (Programmbibliothek zum Informationsschutz - PBSI) "Crypto-Si" verwendet, die von CryptoEx OOO (http://www.cryptoex.ru) entwickelt wurde.

SACHREGISTER

A

Aktivieren
Kindersicherung....171
Anti-Banner
Liste mit verbotenen Banneradressen....162
Anti-Spam
Aggressivitätsstufe....146
Datenbank für Phishing-Webadressen....149
Erweiterung für Microsoft Office Outlook....158
Erweiterung für Microsoft Outlook Express....158
Erweiterung für The Bat!....159
Liste mit verbotenen Absendern....152
Liste mit verbotenen Phrasen....151
Nachrichten für Microsoft Exchange Server....157
Standardparameter wiederherstellen....160
Thunderbird-Erweiterung....160
Training....146
Zusätzliche Merkmale für die Filterung....155
Anti-Spam-Training
mit ausgehenden E-Mails....147
mit Berichten....149
mit Hilfe des Trainingsassistenten....147
mit Hilfe eines Mailprogramms....148

B

Berichte
Anzeigen....76
Flterung....194
in Datei speichern....196
Komponente oder Aufgabe wählen....194
Suche nach Ereignissen....195
Browser-Konfiguration....191

D

Datei-Anti-Virus
Heuristische Analyse....101
Komponente anhalten....98
Reaktion auf eine Bedrohung....101
Schutzbereich....99
Sicherheitsstufe....100
Untersuchung optimieren....103
Untersuchung von zusammengesetzten Dateien....102
Untersuchungsmodus....100
Untersuchungstechnologie....101
Daten löschen
Sichere Umgebung....168
Datenbank für Phishing-Webadressen
Anti-Spam....149
IM-Anti-Virus....118
Web-Anti-Virus....112

E

Echtzeitschutz aktivieren und deaktivieren....57

F

Firewall
- Firewall-Regel....133
- Netzwerkstatus ändern....133
- Paketregel....134
- Priorität einer Regel ändern....135
- Regel für ein Programm....135

Firewall-Regel
- Firewall....133

G

Gemeinsamer Ordner
- Sichere Umgebung....167

H

Heuristische Analyse
- Datei-Anti-Virus....101
- Mail-Anti-Virus....106
- Web-Anti-Virus....112

I

IM-Anti-Virus
- Datenbank für Phishing-Webadressen....118
- Schutzbereich....118

Installationsordner....32

K

Kindersicherung
- Aktivieren und Deaktivieren....171
- Beschränkung für die Verwendung von Computer....174
- Besuch von Webseiten....175
- Download von Dateien aus dem Internet....175
- Korrespondenz über Instant Messenger....176
- Modus für sichere Suche....175
- Parameter exportieren / importieren....172
- Senden von persönlichen Informationen....178
- Start von Programmen....174
- Suche nach Schlüsselwörtern....178
- zeitliche Beschränkung für die Verwendung von Internet....174

Kontextmenü....46

Kontrolle des Zugriffs auf das Programm....83

L

Leistung des Computers....183

Lizenz
- Lizenzvertrag....42
- Programm aktivieren....60

Lizenzverlängerung....61

Löschen
- Programm....40

M

Mail-Anti-Virus
- Anlagenfilterung....106
- Heuristische Analyse....106
- Reaktion auf eine Bedrohung....106
- Schutzbereich....105
- Sicherheitsstufe....105
- Untersuchung von zusammengesetzten Dateien....107

Meldungen 62
Audiosignal deaktivieren 200
Deaktivieren 199
Meldungsarten 200
Senden per E-Mail 200
Modul zur Link-Untersuchung
Web-Anti-Virus 114

N

Netzwerk
Geschützte Verbindungen 139
Zu überwachende Ports 142
Netzwerkmonitor 141
Notfall-CD 73

P

Paketregel
Firewall 134
Proaktiver Schutz
Gruppe mit vertrauenswürdigen Programmen 120
Kontrollregel für gefährliche Aktivität 120
Liste der gefährlichen Aktivität 120
Programmhauptfenster 47
Programmkontrolle
Regel für ein Programm ändern 127
Schutzbereich 130
Startfolge eines Programms 129
Protokollierung
Hochladen der Protokollierungsergebnisse 208
Protokolldatei erstellen 208

Q

Quarantäne und Backup 186

R

Reaktion auf eine Bedrohung
Datei-Anti-Virus 101
Mail-Anti-Virus 106
Virenuntersuchung 88
Web-Anti-Virus 111
Regel für ein Programm
Firewall 135
Regel für ein Programm ändern
Programmkontrolle 127

S

Schutz vor Netzwerkangriffen
Arten der erkennbaren Netzwerkangriffe 137
Computer freigeben 139
Sperrdauer 139
Schutzbereich
Datei-Anti-Virus 99
IM-Anti-Virus 118
Mail-Anti-Virus 105
Programmkontrolle 130
Web-Anti-Virus 116
Selbstschutz für das Programm 185
Sichere Umgebung
Daten löschen 168
Gemeinsamer Ordner 167

Sicherheitsstufe
Datei-Anti-Virus 100
Mail-Anti-Virus 105
Web-Anti-Virus 111
Softwarevoraussetzungen 28
Standardparameter wiederherstellen 76
Anti-Spam 160
Startfolge eines Programms
Programmkontrolle 129
Symbol im Infobereich der Taskleiste 45

U

Untersuchung
Aktion für ein gefundenes Objekt 88
Aufgabenstart 63
automatischer Start einer übersprungenen Aufgabe 86
Benutzerkonto 89
Schwachstellensuche 92
Sicherheitsstufe 86
Typ der zu untersuchenden Objekte 89
Untersuchung optimieren 90
Untersuchung von zusammengesetzten Dateien 90
Untersuchungstechnologien 88
Zeitplan 86
Update
Aus einem lokalen Ordner 94
Proxyserver 96
Regionsoptionen 94
Rollback zum vorherigen Update 96
Updatequelle 93

V

Vertrauenswürdige Zone
Regeln für Ausnahmen 181
vertrauenswürdige Programme 180
Virtuelle Tastatur 68

W

Web-Anti-Virus
Datenbank für Phishing-Webadressen 112
Geo-Filter 115
Heuristische Analyse 112
Modul zur Link-Untersuchung 114
Reaktion auf eine Bedrohung 111
Schutzbereich 116
Sicherheitsstufe 111
Untersuchung optimieren 113
Web-Filter 114

Z

Zeitplan
Update 95
Virensuche 86